Bitdefender®

INTERNET SECURITY 2016

GUIA DO USUÁRIO

Bitdefender Internet Security 2016
Guia do Usuário

Data de Publicação 09/29/2015

Aviso Legal

Índice

INSTALAÇÃO

1. PREPARANDO A INSTALAÇÃO

Antes de instalar o Bitdefender Internet Security 2016, complete estes preparativos para assegurar que a instalação irá ocorrer normalmente:

- Assegure-se que o computador onde deseja instalar o Bitdefender tenha os requisitos mínimos de sistema. Caso o computador não atenda aos requisitos mínimos de sistema, o Bitdefender não será instalado ou caso instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade. Para uma lista completa de requisitos de sistema, por favor consulte "*Requisitos de Sistema*" (p. 3).
- Efetue logon no computador utilizando uma conta de Administrador.
- Remova qualquer outro software similar do seu computador. Rodar dois programas de segurança simultaneamente pode afetar seu funcionamento e causar maiores problemas ao sistema. O Windows Defender será desativado durante a instalação.
- Desabilitar ou remover qualquer programa de firewall que possa estar rodando neste computador. Rodar dois programas de firewall simultaneamente pode afetar a operação deles e causar maiores problemas ao sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu computador esteja conectado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões dos arquivos de aplicativos mais recentes do que as incluídas no pacote de instalação, o Bitdefender irá fazer o download e instalá-las.

2. REQUISITOS DE SISTEMA

Você pode instalar o Bitdefender Internet Security 2016 apenas nos computadores com os seguintes sistemas operacionais:

- Windows 7 com o Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Antes da instalação, certifique-se de que o seu computador cumpre os requisitos mínimos do sistema.

Nota

Para descobrir qual sistema operacional Windows está sendo rodado em seu computador e suas informações de hardware, siga estes passos:

- No **Windows 7**, clique com o botão direito em **Meu Computador** na área de trabalho e depois selecione **Propriedades** no menu.
- No **Windows 8 e Windows 8.1**, na tela Iniciar do Windows, localize Computador (por exemplo, digite "Computador" na tela Iniciar) e clique no ícone com o botão direito. Selecione Propriedades no menu inferior. Procure por informações sobre o tipo do sistema na área do Sistema.
- No **Windows 10**, digite "Sistema" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente. Procure por informações sobre o tipo do sistema na área do Sistema.

2.1. Requisitos mínimos do sistema

- 1 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Processador de 1.6 GHz
- 1 GB de memória (RAM)

2.2. Requisitos de sistema recomendados

- 2 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Intel CORE Duo (2 GHz) ou processador equivalente
- 2 GB de memória (RAM)

2.3. Requisitos de Software

Para conseguir usar o Bitdefender e todos os seus recursos, o seu computador deve cumprir os seguintes requisitos de software:

- Internet Explorer 10 ou superior
- Mozilla Firefox 14 ou superior
- Google Chrome 20 ou superior
- Skype 6.3 ou superior
- Yahoo Messenger 9 ou superior
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (em sistemas de 32 bits)
- Mozilla Thunderbird 14 ou superior

3. INSTALANDO SEU PRODUTO BITDEFENDER

Você pode instalar o Bitdefender utilizando o disco de instalação, ou pelo instalador da web baixado no seu computador da conta Bitdefender Central.

Se sua compra incluir mais de um computador (por exemplo, você comprou o Bitdefender Internet Security 2016 para três computadores), repita o processo de instalação e ative seu produto com a mesma conta em todos os computadores. A conta a ser usada deve ser a mesma que contém sua assinatura ativa do Bitdefender.

3.1. Instale desde Bitdefender Central

Através da conta Bitdefender Central você pode fazer download do kit de instalação correspondente à assinatura comprada. Uma vez que o processo de instalação estiver concluído, o Bitdefender Internet Security 2016 é ativado.

Para baixar o Bitdefender Internet Security 2016 de sua conta Bitdefender Central, siga as seguintes etapas:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**, e então clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Em outro dispositivo**.

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Espere o download ser concluído, depois execute o instalador:

Validando a instalação

O Bitdefender irá primeiro verificar o seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos mínimos para a instalação Bitdefender, você será informado das áreas que precisam de ser melhoradas antes de poder prosseguir.

Se for detectado um programa antivírus incompatível ou uma versão antiga do Bitdefender, será avisado para removê-la do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser preciso reiniciar o seu computador para concluir a remoção dos programas antivírus detectados.

O pacote de instalação do Bitdefender Internet Security 2016 é continuamente atualizado. Clique em **Sim** quando solicitado de forma a permitir que o Bitdefender faça download dos arquivos, assegurando que está instalando a versão mais recente do software.

Nota
Fazer download dos arquivos de instalação pode demorar muito tempo, especialmente se a conexão à Internet for lenta.

Se a instalação estiver validada, o assistente de instalação irá aparecer. Siga estes passos para instalar o Bitdefender Internet Security 2016:

Passo 1 – instalação do Bitdefender

A tela de instalação do Bitdefender permite que você escolha que tipo de instalação deseja fazer.

Para uma experiência de instalação livre de problemas, basta clicar no botão **Instalar**. O Bitdefender será instalado no local padrão com as definições normais e você irá diretamente para a Etapa 3 do assistente.

Caso queira modificar as configurações de instalação, clique em **Personalizar**

Duas tarefas adicionais podem ser realizadas neste passo.

- Por favor, leia o Acordo de Licença de Usuário antes de prosseguir com a instalação. O Acordo de Licença contém os termos e condições sob os quais você pode usar o Bitdefender Internet Security 2016.

  Se não concorda com estes termos, feche a janela. O processo de instalação será abandonado e você sairá da configuração.

- Permitir enviar **Relatórios Anônimos de Utilização**. Ao ativar esta opção, os relatórios que contêm informação sobre como você usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial

para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Note que estes relatórios não contêm dados confidenciais, tais como seu nome ou endereço de IP e que também não serão usados para fins comerciais.

Passo 2 - Personalizar definições da instalação

Nota
Este passo apenas aparece caso tenha optado por personalizar a instalação durante o passo anterior.

As seguintes opções estão disponíveis:

Instalar caminho
Por padrão, o Bitdefender Internet Security 2016 será instalado em C:\Arquivos de Programa\Bitdefender\Bitdefender 2016\. Se deseja alterar o caminho de instalação, clique em **Alterar** e selecione a pasta na qual pretende que o Bitdefender seja instalado.

Configurar Definições de Proxy
O Bitdefender Internet Security 2016 requer o acesso à Internet para registro do produto, baixar atualizações de segurança e de produtos, componentes de detecção na nuvem, etc. Se usar uma conexão por proxy em vez de uma conexão direta à Internet, deve selecionar esta opção e configurar as definições.

As definições podem ser importadas do navegador padrão ou você pode introduzi-las manualmente.

Clique em **Instalar** para confirmar suas preferências e iniciar a instalação. Caso mude de ideia, clique no botão **Utilizar padrão** correspondente.

Passo 3 - Evolução da instalação

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

As áreas críticas do seu sistema são analisadas em busca de vírus, as últimas versões dos arquivos do aplicativo são baixadas e instaladas, e os serviços do Bitdefendersão iniciados. Este passo pode demorar alguns minutos.

Passo 4 - Instalação terminada

Seu produto Bitdefender foi instalado com sucesso.

É apresentado um resumo da instalação. Se tiver sido detectado malware ativo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique **OK** para continuar.

Passo 5 - Introdução

Na tela Introdução você pode ver a validade da sua assinatura.

Duas tarefas adicionais podem ser realizadas neste passo.

- Compre uma nova assinatura – este link o(a) redireciona para a página do Bitdefender de onde você pode comprar uma nova assinatura.
- Tenho um código de ativação – este link o(a) redireciona para sua conta Bitdefender Central. Clique em **CÓDIGO DE ATIVAÇÃO** na janela Minha Assinatura que aparece. Digite seu código de ativação, depois clique em **MANDAR**.

Clique em **Finalizar** para acessar a interface do Bitdefender Internet Security 2016.

3.2. Instale a partir do disco de instalação.

Para instalar o Bitdefender a partir do disco de instalação, insira o disco na unidade ótica.

Uma tela de instalação deve ser exibida em alguns instantes. Siga as instruções para iniciar a instalação.

Nota

A tela de instalação fornece a opção de copiar o pacote de instalação do disco de instalação para um dispositivo de armazenamento USB. Isto é útil se você precisar instalar o Bitdefender em um computador que não possui uma unidade de disco (por exemplo, em um netbook). Insira o dispositivo no drive USB e então clique **Copiar para USB**. Depois, vá para o computador sem a unidade de disco, insira o dispositivo de armazenamento na unidade USB e clique duas vezes runsetup.exe na pasta onde você salvou o pacote de instalação.

Se a tela de instalação não aparecer, use o Windows Explorer para procurar no diretório da raiz do disco e clique duas vezes no arquivo autorun.exe.

Validando a instalação

O Bitdefender irá primeiro verificar o seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos mínimos para a instalação Bitdefender, você será informado das áreas que precisam de ser melhoradas antes de poder prosseguir.

Se for detectado um programa antivírus incompatível ou uma versão antiga do Bitdefender, será avisado para removê-la do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser preciso reiniciar o seu computador para concluir a remoção dos programas antivírus detectados.

O pacote de instalação do Bitdefender Internet Security 2016 é continuamente atualizado. Clique em **Sim** quando solicitado de forma a permitir que o Bitdefender faça download dos arquivos, assegurando que está instalando a versão mais recente do software.

Nota
Fazer download dos arquivos de instalação pode demorar muito tempo, especialmente se a conexão à Internet for lenta.

Se a instalação estiver validada, o assistente de instalação irá aparecer. Siga estes passos para instalar o Bitdefender Internet Security 2016:

Passo 1 – instalação do Bitdefender

A tela de instalação do Bitdefender permite que você escolha que tipo de instalação deseja fazer.

Para uma experiência de instalação livre de problemas, basta clicar no botão **Instalar**. O Bitdefender será instalado no local padrão com as definições normais e você irá diretamente para a Etapa 3 do assistente.

Caso queira modificar as configurações de instalação, clique em **Personalizar**

Duas tarefas adicionais podem ser realizadas neste passo.

- Leia o Acordo de Licença de Usuário antes de iniciar a instalação. O Acordo de Licença contém os termos e condições sob os quais você pode usar o Bitdefender Internet Security 2016.

  Se não concorda com estes termos, feche a janela. O processo de instalação será abandonado e você sairá da configuração.

- Selecione **Enviar relatórios anônimos de uso**. Ao ativar esta opção, os relatórios que contêm informação sobre como você usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Observe que esses relatórios contêm dados não confidenciais, como seu nome ou endereço de IP, e que eles não serão usados para fins comerciais.

Passo 2 - Personalizar definições da instalação

Nota

Este passo apenas aparece caso tenha optado por personalizar a instalação durante o passo anterior.

As seguintes opções estão disponíveis:

Instalar caminho

Por padrão, o Bitdefender Internet Security 2016 será instalado em C:\Arquivos de Programa\Bitdefender\Bitdefender 2016\. Se deseja alterar o caminho de instalação, clique em **Alterar** e selecione a pasta na qual pretende que o Bitdefender seja instalado.

Configurar Definições de Proxy

O Bitdefender Internet Security 2016 requer acesso à Internet para a ativação do produto, download de atualizações de segurança e de produto, componentes de detecção na nuvem, etc. Se usar uma conexão por proxy em vez de uma conexão direta à Internet, deve selecionar esta opção e configurar as definições.

As definições podem ser importadas do navegador padrão ou você pode introduzi-las manualmente.

Clique em **Instalar** para confirmar suas preferências e iniciar a instalação. Caso mude de ideia, clique no botão **Utilizar padrão** correspondente.

Passo 3 - Evolução da instalação

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

As áreas críticas do seu sistema são analisadas em busca de vírus, as últimas versões dos arquivos do aplicativo são baixadas e instaladas, e os serviços do Bitdefendersão iniciados. Este passo pode demorar alguns minutos.

Passo 4 - Instalação terminada

É apresentado um resumo da instalação. Se tiver sido detectado malware ativo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique **OK** para continuar.

Passo 5 - Bitdefender Central

Após concluir a configuração inicial, a janela Bitdefender Central aparece. Uma conta Bitdefender Central é necessária para ativar o produto e usar suas ferramentas online. Para mais informações, por favor consulte “*Bitdefender Central*” (p. 38).

Proceda de acordo com sua situação.

Já tenho uma conta Bitdefender Central

Digite o endereço de e-mail e a senha da sua conta Bitdefender Central, e então clique em **ENTRAR**.
Se esqueceu a senha de sua conta ou quer redefinir a senha anterior, clique no link **Redefinir senha**. Digite seu endereço de e-mail, depois clique no botão **REDEFINIR SENHA**.

Quero criar uma conta Bitdefender Central

Para criar uma conta Bitdefender Central, clique no link **Cadastrar-se** localizado na parte inferior da janela. Digite a informação solicitada nos campos correspondentes, e então clique no botão **CRIAR CONTA**.

Os dados que nos fornecer serão mantidos confidenciais.

A senha deve possuir no mínimo 8 caracteres e incluir um número.

Nota

Uma vez a conta criada, você pode usar o endereço de e-mail fornecido e a senha para fazer o login na sua conta em https://central.bitdefender.com.

Passo 6 - Introdução

Na tela Introdução você pode ver a validade da sua assinatura.

Duas tarefas adicionais podem ser realizadas neste passo.

- Compre uma nova assinatura – este link o(a) redireciona para a página do Bitdefender de onde você pode comprar uma nova assinatura.

- Tenho um código de ativação – este link o(a) redireciona para sua conta Bitdefender Central. Clique em **CÓDIGO DE ATIVAÇÃO** na janela Minha Assinatura que aparece. Digite seu código, depois clique em **MANDAR**.

Clique em **Finalizar** para acessar a interface do Bitdefender Internet Security 2016.

INTRODUÇÃO

4. O BÁSICO

Assim que instalar o Bitdefender Internet Security 2016, o seu computador fica protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia) e ameaças da Internet (tais como hackers, phishing e spam).

O aplicativo usa a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise do antimalware. Ele funciona através da aprendizagem dos padrões de uso de seus aplicativos de sistema para saber o que e quando analisar, minimizando o impacto no desempenho do sistema.

Pode ligar o Autopilot para desfrutar da segurança automática e silenciosa, onde não é necessário configurar absolutamente nada. No entanto, poderá querer usufruir das definições do Bitdefender para optimizar e melhorar a sua proteção.

Enquanto você trabalha, joga ou assiste filmes, Bitdefender pode lhe oferecer uma experiência de usuário contínua, adiando as tarefas de manutenção, eliminando as interrupções e ajustando os efeitos visuais do sistema. Você pode se beneficiar de tudo isso, ativando e configurando os Perfis.

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Detalhes sobre as ações tomadas e informações sobre o funcionamento do programa encontram-se disponíveis na janela Eventos. Para mais informações, por favor consulte "*Eventos*" (p. 17).

De vez em quando, deve abrir o Bitdefender e corrigir as incidências existentes. Você pode ter que configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger seu computador e seus dados.

Para usar as ferramentas online do Bitdefender Internet Security 2016 e gerenciar suas assinaturas e dispositivos, acesse sua conta Bitdefender Central. Para mais informações, por favor consulte "*Bitdefender Central*" (p. 38).

A seção "Como" (p. 47) é onde você irá encontrar instruções passo-a-passo sobre como realizar as tarefas mais comuns. Caso haja incidências durante o uso do Bitdefender, consulte a "*Resolvendo incidências comuns*" (p. 167) seção de possíveis soluções para os problemas mais comuns.

4.1. Abrindo a janela do Bitdefender

Para acessar a interface principal do Bitdefender Internet Security 2016, siga os passos abaixo:

- No **Windows 7**:
  1. Clique **Iniciar** e acesse **Todos os Programas**.
  2. Clique em **Bitdefender 2016**.
  3. Clique em **Bitdefender Internet Security 2016** ou, mais rápido, clique duas vezes no ícone do Bitdefender B na barra de sistema.
- No **Windows 8 e Windows 8.1**:

  A partir da tela Iniciar do Windows, localize Bitdefender Internet Security 2016 (por exemplo, você pode começar a digitar "Bitdefender" diretamente no menu Iniciar) e então clicar em seu ícone. Como alternativa, abra o aplicativo na Área de Trabalho e, em seguida, clique duas vezes no ícone do Bitdefender B na barra do sistema.
- No **Windows 10**:

  Digite "Bitdefender" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente. Ou então clique duas vezes no ícone do Bitdefender B na área de notificação.

Para mais informações sobre a janela e ícone do Bitdefender na bandeja do sistema, por favor consulte *"Interface Bitdefender"* (p. 25).

4.2. Corrigindo os problemas

O Bitdefenderutiliza um sistema de rastreio de problemas para detectar e lheinformar sobre os problemas que podem afetar a segurança do seu computador edados. Por padrão, ele irá monitorar apenas uma série de problemas que são considerados muito importantes. De qualquer forma você pode configurá-lo conforme suas necessidades, escolhendo sobre quais problemas específicos você deseja ser notificado.

As incidências detectadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco à segurança. Estão organizadas em duas categorias:

- **Questões críticas** - impedem que o Bitdefender proteja você contra malware ou represente um grande risco à segurança.

- **Incidências menores (não críticas)** - podem afetar a sua proteção num futuro próximo.

O ícone Bitdefender na bandeja do sistema indica incidências pendentes alterando a sua cor conforme indicado a seguir:

Questões críticas estão afetando a segurança do seu sistema. Requerem sua atenção imediata e devem ser corrigidos assim que possível.
Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.

Também, se você mover o cursor do mouse sobre o ícone, um pop-up irá confirmar a existência de problemas pendentes.

Quando você abre a interface do Bitdefender, a área de status de segurança na barra de ferramentas superior indicará a natureza dos problemas que afetam seu sistema.

4.2.1. Assistente de Correção de todos os Problemas

Para resolver as incidências detectadas siga o assistente **Reparar todas as incidências**.

1. Para abrir o assistente, faça qualquer um dos seguintes:
   - Clique com o botão direito do mouse no ícone do Bitdefender na bandeja do sistema e selecione **Ver problemas de segurança**.
   - Abra a interface do Bitdefender e clique em qualquer lugar dentro da área de status de segurança na barra de ferramentas superior (por exemplo, você pode clicar no link **Corrigir todas as incidências!**).
2. Você pode verificar as incidências que afetam a segurança do seu computador e dos dados. Todas ocorrências atuais estão selecionadas para serem corrigidas.

   Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente. Será solicitado que você especifique por quanto tempo pretende adiar a correção do problema. Escolha a opção desejada no menu e clique em **OK**. Para deixar de monitorar a categoria de problema respectiva, escolha **Permanentemente**.

   O status de incidências será alterado para **Adiado** e nenhuma ação será tomada para corrigir o problema.

3. Para reparar todas as incidências selecionadas, clique em **Reparar.** Algumas ocorrências são corrigidas imediatamente. Para outras, um assistente ajudará a corrigir

As questões que este assistente ajuda você a corrigir podem ser agrupadas em cinco categorias principais:

- **Configurações de segurança desativadas.** Tais problemas são corrigidos imediatamente, ao permitir as respectivas definições de segurança.
- **Tarefas preventivas de segurança que você precisa executar.** Ao fixar tais problemas, um assistente ajuda-o a concluir com êxito a tarefa.

4.2.2. Configure o alerta de status

O Bitdefender informa quando são detectadas incidências no funcionamento dos seguintes componentes do programa:

- Firewall
- Antispam
- Antivírus
- Atualizar
- Segurança do Navegador

Pode configurar o sistema de alerta para melhor responder às suas necessidades de segurança escolhendo as incidências específicas sobre as quais pretende receber informações. Siga esses passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a aba **Avançado**.
3. Clique no link **Configurar estado dos alertas**.
4. Clique nos botões para ligar ou desligar os alertas de estado de acordo com as suas preferências.

4.3. Eventos

O Bitdefender mantém um registro detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que ocorre algo relevante à segurança do seu sistema ou dados, uma nova mensagem é adicionada aos Eventos do Bitdefender, de forma similar a um novo e-mail que aparece na sua Caixa de Entrada.

Os eventos são uma ferramenta importante na monitoração e gestão da proteção do seu Bitdefender. Por exemplo, você pode facilmente verificar se a atualização foi executada com sucesso, se foi encontrado algum malware no seu computador. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para acessar ao registro (log) dos Eventos, faça o seguinte:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.

As mensagens são agrupadas conforme o módulo do Bitdefender cuja atividade se relacione com:

- **Atualizar**
- **Antivírus**
- **Proteção da Internet**
- **Vulnerabilidade**
- **Firewall**
- **Detecção de Invasão**
- **Antispam**
- **Proteção contra Ransomware**

Sempre que um evento ocorrer, um ponto pode ser visto no ícone no topo da interface do Bitdefender.

Encontra-se disponível uma lista de eventos para cada categoria. Para obter informações sobre um evento em particular da lista, clique no ícone e selecione **Eventos** no menu suspenso. As informações sobre o evento são exibidas na lateral direita da janela. Cada evento surge com a seguinte informação: uma breve descrição, a ação do Bitdefender quando este ocorreu, e a data e hora em que ocorreu. Podem ser fornecidas opções para tomar outras medidas, caso seja necessário.

Você poderá filtrar eventos por importância e ordem de acontecimento. Há três tipos de eventos filtrados por importância, sendo cada tipo indicado com um ícone específico:

■ Os eventos **Críticos** indicam problemas críticos. Verifique-os imediatamente.
■ O eventos de **Aviso** indicam incidências não críticas. Deve verificá-las e repará-las quando tiver oportunidade.

- Eventos de **Informação** indicam operações bem sucedidas.

Para visualizar eventos que ocorreram em determinado período de tempo, selecione o período desejado no campo correspondente.

Para o ajuda-lo a administrar facilmente os eventos registrados, cada seção da janela de Eventos oferece opções para eliminar ou marcar como lidos todos os eventos daquela seção.

4.4. Automático

Para todos os usuários que desejam nada mais da sua solução de segurança do que serem protegidos sem serem incomodados, a Bitdefender Internet Security 2016 foi concebida com um modo Autopilot.

No Autopilot, o Bitdefender aplica uma configuração de segurança otimizada e toma todas as decisões relacionadas à segurança por você. Isto significa que não verá pop-ups nem alertas e não terá de configurar quaisquer definições.

No modo Autopilot, o Bitdefender repara automaticamente incidências críticas, ativa e gerencia discretamente:

- Proteção antivírus, proporcionada pela análise no acesso e análise contínua.
- Proteção de Firewall.
- Proteção da Internet.
- Atualizações Automáticas.

Para ligar ou desligar o Autopilot, siga os seguintes passos:

1. Clique no botão **Autopilot** na barra de ferramentas superior da interface do Bitdefender.

Enquanto o Autopilot estiver ligado, o ícone Bitdefender na área de notificação mudará para .

Importante

Enquanto o Autopilot estiver ligado, em caso de modificação de alguma das definições, este será desligado.

Para ver o histórico das ações executadas pelo Bitdefender enquanto o Autopilot estava ligado, abra a janela Eventos.

4.5. Perfis e Modo de Bateria

Algumas atividades do computador, como jogos on-line ou apresentações de vídeo, requerem maior capacidade de resposta, alta performance e nenhuma interrupção do sistema. Quando seu laptop esta operando funcionando com a bateria, o melhor é que operações desnecessárias, que consomem energia, sejam adiadas até que o laptop esteja ligado a uma rede de energia.

Para se adaptar a estas situações particulares, o Antivirus Bitdefender 2010 inclui dois modos especiais de operação:

- Perfis
- Modo de Bateria

4.5.1. Perfis

Os Perfis do Bitdefender atribuem mais recursos do sistema para os aplicativos em execução, modificando temporariamente as configurações de proteção e ajustando a configuração do sistema. Consequentemente, o impacto do sistema na sua atividade é minimizado.

Para se adaptar a diferentes atividades, o Bitdefender vem com os seguintes perfis:

Perfil de Trabalho
: Otimiza a sua eficiência de trabalho ao identificar e ajustar as configurações de produto e de sistema.

Perfil de Filme
: Melhora os efeitos visuais e elimina as interrupções ao assistir filmes.

Perfil de Jogo
: Melhora efeitos visuais e elimina as interrupções ao jogar.

Ativando e desativando os perfis

Para ativar ou desativar os perfis, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione a aba **Configurações de Perfis**.

5. Ative ou desative os perfis clicando no botão correspondente.

Configure o Autopilot para monitorar os perfis

Para uma experiência de usuário intuitiva, você pode configurar o Autopilot para gerenciar o seu perfil de trabalho. Neste modo, o Bitdefender detecta automaticamente a sua atividade e realiza e aplica configurações de otimização do produto.

Para permitir que o Autopilot gerencie os perfis, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione a aba **Configurações de Perfis**.
5. Marque a caixa **Permitir que o Autopilot administre meus perfis**.

Caso você não queira que seu Perfil seja controlado automaticamente, deixe a caixa desmarcada e escolha-o a partir da lista **PERFIS** na interface do Bitdefender.

Para obter mais informações sobre Perfis, consulte"*Perfis*" (p. 160)

4.5.2. Modo de Bateria

Modo de Bateria é projetado especialmente para usuários de laptops e tablets. O seu objetivo é minimizar o impacto do sistema e do Bitdefender no consumo de energia quando o nível de bateria estiver abaixo do nível selecionado por você.

As configurações de produto a seguir são aplicadas quando o Bitdefender opera em Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.
- As análises programadas são adiadas.
- O Dispositivo de Segurança é desligado.

O Bitdefender detecta quando o seu laptop está ligado na bateria e dependendo do nível de carga da bateria, ele automaticamente entra em Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do

Modo de Bateria ao detectar que o laptop está conectado com um cabo de energia.

Para ativar ou desativar o Modo de Bateria, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois selecione a aba **Modo Bateria**.
4. Ative ou desative o Modo de Bateria automático clicando no botão correspondente.

   Arraste o cursor correspondente pela escala para definir quando o sistema deve começar a operar em Modo de Bateria. Por padrão, o modo é ativado quando o nível da bateria cai abaixo de 30%.

Nota
O Modo de Bateria é habilitado por padrão em notebooks e tablets.

Configurando o Modo de Bateria

Para configurar o Modo de Bateria, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois selecione a aba **Modo Bateria**.
4. Ative a função clicando no botão correspondente.
5. Clique no botão **Configurar**.
6. Escolha os ajustes de sistema que serão aplicados selecionando as seguintes opções:
   - Otimize as configurações do produto para o Modo de bateria.
   - Adie programas em segundo plano e tarefas de manutenção.
   - Adie as Atualizações Automáticas do Windows.
   - Ajuste as configurações do plano de energia para o Modo de bateria.
   - Desative os dispositivos externos e portas de rede.
7. Clique **Salvar** para salvar as alterações e fechar a janela.

4.6. Configurações de proteção da senha do Bitdefender

Se você não é a única pessoa a usar esse computador com direitos de administrador, é recomendado que você proteja suas configurações do Bitdefender com uma senha.

Para configurar a proteção de senha para as definições do Bitdefender, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Configurações Gerais**, selecione a aba **Configurações Gerais**.
3. Ative a Proteção por senha clicando no botão correspondente.
4. Insira a senha nos dois campos e depois clique em **OK**. A senha deve conter no mínimo 8 caracteres.

Depois de definir uma senha, se alguém tentar mudar as definições do Bitdefender terá primeiro de fornecer a senha.

Importante

Memorize a sua senha ou guarde-a em um local seguro. Se esquecer a senha, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Para remover a proteção da senha, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Configurações Gerais**, selecione a aba **Configurações Gerais**.
3. Desligue a proteção por senha ao clicar no botão. Digite a nova senha e depois clique em **OK**.

Nota

Para alterar a senha para o seu produto, clique no link **Alterar Senha**.

4.7. Relatórios de utilização anônimos

Por predefinição, o Bitdefender envia relatórios que contêm informação sobre como usá-lo nos servidores Bitdefender. Esta informação é essencial

para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Note que estes relatórios não contêm dados confidenciais, tais como seu nome ou endereço de IP e que também não serão usados para fins comerciais.

Caso queira parar de enviar Relatórios Anônimos de utilização, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a aba **Avançado**.
3. Clique no botão para desligar os Relatórios Anônimos de utilização.

4.8. Ofertas especiais e notificações de produto

Quando as ofertas promocionais forem disponibilizadas, o produto Bitdefender está configurado para notificá-lo através de uma janela. Isso lhe dará a oportunidade de aproveitar preços vantajosos e manter os dispositivos protegidos por um período mais longo.

Adicionalmente, as notificações de produto poderão aparecer quando o usuário fizer alterações no produto.

Para ativar ou desativar ofertas especiais e notificações de produto, siga esses passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Configurações Gerais**, selecione a aba **Configurações Gerais**.
3. Ative ou desative ofertas especiais e notificações de produto clicando no botão correspondente.

As opções de ofertas especiais e de notificações de produto estão ativadas por padrão.

Nota

Após desabilitar notificações de ofertas especiais e produtos, o Bitdefender continuará a mantê-lo informado sobre ofertas especiais quando você usar uma versão de teste, quando sua assinatura for expirar ou quando você estiver usando uma versão expirada do produto.

5. INTERFACE BITDEFENDER

Bitdefender Internet Security 2016 vai de encontro às necessidades tanto de iniciantes como de pessoas mais técnicas. Sua interface gráfica do usuário foi projetada para qualquer categoria de usuário.

Para ver o status do produto e realizar tarefas essenciais, o Bitdefender ícone na bandeja do sistema está disponível a qualquer momento.

A janela principal permite o acesso a informações importantes do produto, módulos do programa, e permite que você realize tarefas comuns. Na tela principal, você pode acessar os módulos do Bitdefender para configuração detalhada e tarefas administrativas avançadas, e controlar o comportamento do produto utilizando o Autopilot e Perfis.

Se deseja manter uma vigilância constante na informação essencial de segurança e ter um acesso rápido a definições chave, adicione o Dispositivo Segurança ao seu ambiente de trabalho.

5.1. Ícone da bandeja do sistema

Para gerenciar todo o produto mais rapidamente, você pode usar o ícone do Bitdefender na área de notificação.

Nota

Pode ser que o ícone do Bitdefender não esteja visível o tempo todo. Para fazer com que o ícone sempre apareça, faça o seguinte:

- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Clique na seta no canto inferior direito da tela.
  2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.
  3. Selecione a opção **Mostrar ícones e notificações** para o ícone do **Agente do Bitdefender Agent**.
- No **Windows 10**:
  1. Clique com o botão direito na barra de tarefas e selecione **Propriedades**.
  2. Clique em **Personalizar** na janela da barra de tarefas.
  3. Clique no link de **Selecione quais ícones aparecem na barra de ferramentas** na janela de **Notificações e ações**.
  4. Ative o botão ao lado do **Agente do Bitdefender**.

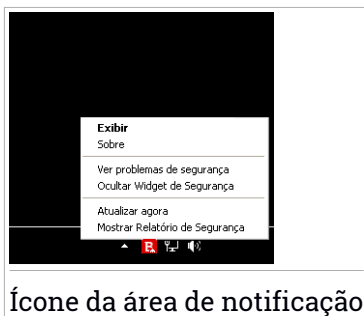
Se clicar duas vezes neste ícone, o Bitdefender irá abrir. Além disso, clicando com o botão direito do mouse no menu contextual, permitirá você gerenciar o produto Bitdefendermais rapidamente.

Ícone da área de notificação

- **Exibir** - abre a janela principal do Bitdefender.
- **Sobre** - abre uma janela onde pode ver informação sobre o Bitdefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Ver problemas de segurança** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, não há problemas a serem corrigidos. Para informação detalhada, por favor consulte em “*Corrigindo os problemas*” (p. 15).
- **Ocultar / Exibir Dispositivo Segurança** - ativa / desativa Dispositivo Segurança.
- **Atualizar agora** - realiza uma atualização imediata. Você pode acompanhar o status de atualizações no painel de Atualizações na janela do Bitdefender.
- **Mostrar Relatório de Segurança** - abre uma janela onde você pode visualizar o status semanal e recomendações para seu sistema. Você pode seguir as recomendações para melhorar a segurança do seu sistema.

O ícone da área de notificação do Bitdefender lhe informa quando problemas afetam seu computador ou como o produto é operado, ao mostrar um símbolo especial, como segue:

Questões críticas estão afetando a segurança do seu sistema. Requerem sua atenção imediata e devem ser corrigidos assim que possível.
Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.
O Autopilot Bitdefender está ativado.

Se o Bitdefender não estiver funcionando, o ícone da bandeja do sistema aparece sobre um fundo cinza: . Isso geralmente ocorre quando a chave de licença expira. Isso pode ocorrer também quando os serviços do Bitdefender não estão respondendo ou quando outros erros afetam a operação normal do Bitdefender.

5.2. Janela Principal

A tela principal do Bitdefender permite que você realize tarefas comuns, resolva problemas de segurança rapidamente, visualize informações sobre a operação do produto e acesse os painéis para alterar as configurações do produto. Tudo se encontra a apenas uns cliques de distância.

A janela está organizada em duas áreas principais:

Barra de ferramentas superior
: Aqui você pode verificar o estado de segurança do seu computador, configurar o comportamento do Bitdefender em casos especiais e acessar tarefas importantes.

Área dos botões de ação
: Aqui você pode acessar a conta do painel de controle Bitdefender Central e realizar diferentes tarefas para manter seu sistema protegido e funcionando na velocidade ideal.

O ícone no canto inferior esquerdo da interface principal lhe dá acesso aos módulos do produto para que você possa iniciar a configuração do produto.

O ícone no topo da interface principal permite que você controle sua conta e acesse as funções online do seu produto no painel de controle da conta. Aqui você pode acessar os Eventos, o Relatório de Segurança semanal, e a página de Ajuda e Suporte.

Link	Descrição
Número de dias restantes	O tempo restante até o fim de sua assinatura é exibido. Clique no link para abrir a janela onde poderá ver mais informações sobre sua chave de licença ou registrar o seu produto com a nova chave de licença.

5.2.1. Barra de ferramentas superior

A barra de ferramentas superior contém os seguintes elementos:

- A **Área de Estado da Segurança** do lado esquerdo da barra de ferramentas, informa se existem incidências a afetar a segurança do seu computador e ajuda a repará-las.

A cor da área de status da segurança muda dependendo das incidências detectadas e são apresentadas diferentes mensagens:

- **A área está colorida de verde.** Não existem incidências para resolver. Seu computador e dados estão protegidos.
- **A área está colorida de amarelo.** Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.
- **A área está colorida de vermelho.** Questões críticas estão afetando a segurança do seu sistema. Você deve resolver os problemas detectados imediatamente.

Ao clicar em qualquer lugar na área de status de segurança, você poderá cessar um assistente que irá ajudar a facilmente remover quaisquer ameaças de seu computador. Para informação detalhada, por favor consulte em “*Corrigindo os problemas*” (p. 15).

- O **Autopilot** permite que você execute o Autopilot e desfrute da segurança de forma completamente silenciosa. Para informação detalhada, por favor consulte em “*Automático*” (p. 19).
- Os **Perfis** permitem que você trabalhe, jogue ou assista filmes economizando tempo ao configurar o sistema para adiar tarefas de manutenção. Para informação detalhada, por favor consulte em “*Perfis*” (p. 160).

5.2.2. Botões de ação

Você pode usar os botões de ação para acessar rapidamente a sua conta Bitdefender Central e realizar tarefas importantes.

Os botões de ação disponíveis nesta área são:

- **Ir a Bitdefender Central**. Acesse sua conta Bitdefender Central para verificar suas assinaturas e realizar tarefas de segurança nos dispositivos que você controla.
- **Quick Scan**. Faça uma análise rápida para garantir que seu computador esteja livre de vírus.
- **Analisar Vulnerabilidade**. Verifique seu computador para identificar vulnerabilidades e assegurar que todos os aplicativos instalados, além do sistema operacional, estejam atualizados e funcionando corretamente.
- **Safepay**. Abra o Bitdefender Safepay™ para proteger seus dados privados ao realizar transações online.

- **Atualizar**. Atualize o seu Bitdefender para garantir que você tenha as assinaturas de malware mais recentes.

5.3. Os módulos do Bitdefender

O Bitdefender vem com vários módulos úteis para protegê-lo enquanto você trabalha, navega na web, joga ou realiza pagamentos online.

Sempre que você acessar os módulos ou começar a configurar seu produto, clique no ícone no campo inferior esquerdo da interface do Bitdefender.

Os módulos são separados em três abas, com base nas funções que oferecem:

- Proteção
- Privacidade
- Ferramentas

5.3.1. Proteção

Nesta aba, você pode configurar seu nível de segurança, gerenciar amigos e spammers, visualizar e editar as configurações de rede e determinar que vulnerabilidades devem ser corrigidas.

Os módulos que podem ser gerenciados no Painel de Proteção são:

Antivírus

A proteção antivirus é a base da sua segurança. O Bitdefender protege em tempo real e a pedido contra todos os tipos de malware, tais como vírus, trojans, spyware, adware, etc.

Do módulo Antivírus, você pode acessar facilmente as seguintes tarefas de análise:

- Quick Scan
- Análise do Sistema
- Gerenciar Verificações
- Modo de Recuperação

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, por favor consulte "*Proteção Antivírus*" (p. 80).

Proteção da Internet

A proteção da internet ajuda você a manter-se protegido contra ataques de phishing, tentativas de fraude e vazamento de dados pessoais enquanto navega na Internet.

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade na rede, consulte *"Proteção da Internet"* (p. 115).

Vulnerabilidade

O módulo de Vulnerabilidade ajuda você a manter o sistema operacional e os aplicativos que você usa regularmente atualizados.

Clique em **Análise de Vulnerabilidade** no módulo de Vulnerabilidade para começar a identificar atualizações críticas do Windows, atualizações de aplicativos e senhas fracas em contas do Windows.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte *"Vulnerabilidade"* (p. 119).

Firewall

A firewall protege você enquanto está conectado às redes e à Internet, através da filtragem de todas as tentativas de conexão.

Para mais informações sobre configuração de firewall, consulte *"Firewall"* (p. 123).

Detecção de Invasão

A Detecção de Invasão analisa as atividades de sistema e de rede para comportamentos incomuns e possíveis ataques.

Para mais informações sobre como configurar a Detecção de Invasão para proteger a atividade de seu sistema e de sua rede, consulte *"Detecção de Invasão"* (p. 131).

Antispam

O módulo antispam do Bitdefender assegura que a sua Caixa de Entrada permaneça livre de e-mails indesejados através da filtragem do tráfego de e-mail POP3.

Para mais informações sobre a proteção antispam, consulte *"Antispam"* (p. 105).

Proteção contra Ransomware

O módulo de Proteção contra Ransomwares protege seus arquivos pessoais contra ataques de chantagistas.

Para mais informações sobre como configurar a Proteção contra Ransomwares para proteger seu sistema contra ataques de ransomware, acesse *"Proteção contra Ransomware"* (p. 132).

5.3.2. Privacidade

Na aba Privacidade, você pode encriptar seus dados pessoais, proteger suas transações online, manter sua navegação segura e proteger seus filhos ao visualizar e restringir sua atividade online.

Os módulos que podem ser gerenciados no Painel de Privacidade são:

Proteção de Dados

O módulo de Proteção de dados permite que você apague arquivos permanentemente.
Clique no **Destruidor de Arquivos** sob o módulo de proteção de dados para iniciar um assistente que lhe permitirá eliminar completamente os arquivos de seu sistema.

Para mais informações sobre como configurar a Proteção de Dados, consulte *"Proteção de Dados"* (p. 117).

Gerenciador de Senhas

O Gerenciador de Senhas do Bitdefender o ajuda a lembrar as suas senhas, protege sua privacidade e fornece uma navegação segura.

No módulo Gerenciador de Senhas você pode selecionar as seguintes tarefas:

- **Abrir Carteira** - abre a base de dados existente da Carteira.
- **Bloquear carteira** - bloqueia as informações existentes na Carteira.
- **Exportar Carteira** - permite que você salve a base de dados atual para um local no seu sistema.
- **Criar nova Carteira** - inicia um assistente que permite que você crie uma nova base de dados da Carteira.

Para mais informações sobre a configuração do Gerenciador de Senhas, acesse *"Proteção do Gerenciador de Senhas para suas credenciais"* (p. 140).

Safepay

O navegador Bitdefender Safepay™ ajuda a manter a sua atividade bancária on-line, compras on-line e qualquer outro tipo de transação on-line, privada e segura.

Clique no botão de ação **Safepay** na interface do Bitdefender para começar a realizar transações online em um ambiente seguro.

Para mais informações sobre o Bitdefender Safepay™, consulte *"Segurança Safepay para transações online"* (p. 135).

Consultor Parental

O Consultor Parental do Bitdefender permite que você monitore o que seu filho está fazendo no computador. Caso haja conteúdo inapropriado, você pode decidir restringir o seu acesso à Internet ou a aplicativos específicos.

Clique em **Configurar** no módulo de Consultor Parental para iniciar a configuração das contas do Windows de seus filhos e começar a monitorar suas senhas onde quer que estejam.

Para mais informações sobre a configuração do Consultor Parental, acesse *"Consultor Parental"* (p. 148).

5.3.3. Ferramentas

Na aba Ferramentas, você pode configurar seu perfil de trabalho.

Os módulos que você pode controlar na aba de Ferramentas são:

Perfis

Os Perfis do Bitdefender ajudam você a ter uma experiência de usuário simplificada enquanto trabalha, assiste um filme ou joga, através do monitoramento do produto e das ferramentas de trabalho do sistema. Clique em **Ativar agora** na barra de ferramentas superior da interface do Bitdefender para começar a usar esse recurso.

O Bitdefender permite que você configure os seguintes perfis:

- Perfil de Trabalho
- Perfil de Filme
- Perfil de Jogo

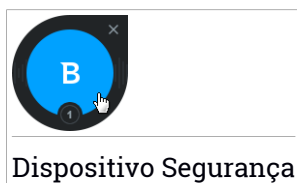
Para mais informações sobre como configurar o módulo dos Perfis, consulte *"Perfis"* (p. 160).

5.4. Dispositivo Segurança

Dispositivo Segurança é a forma rápida e fácil de controlar o Bitdefender Internet Security 2016. Adicionar este dispositivo pequeno e não intrusivo

à sua área de trabalho permite ver informações criticas e realizar tarefas importantes a qualquer instante:

- abrir a janela principal do Bitdefender.
- monitorar a atividade de análise em tempo-real.
- monitorar o status de segurança do seu sistema e reparar qualquer incidência existente.
- ver quando uma atualização está em andamento.
- visualizar notificações e acessar os mais recentes eventos relatados pelo Bitdefender.
- analisar arquivos ou pastas ao arrastar e soltar um ou vários itens sobre o dispositivo.

Dispositivo Segurança

O status geral de segurança do seu computador é mostrado **no centro** do dispositivo. O estado é indicado pela cor e forma do ícone exibido nessa área.

Questões críticas estão afetando a segurança do seu sistema.

Requerem sua atenção imediata e devem ser corrigidos assim que possível. Clique no ícone de status para começar a reparar as incidências reportadas.

Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade. Clique no ícone de status para começar a reparar as incidências reportadas.

Seu sistema está protegido

Quando uma tarefa de análise a-pedido está em progresso, este ícone animado é apresentado.

Quando são reportadas incidências, clique no ícone de status para ativar o assistente de Reparação de Incidências.

O lado inferior do dispositivo exibe o contador de eventos não lidos (o número de eventos importantes reportados pelo Bitdefender, caso haja algum). Clique no contador de eventos, por exemplo, para um evento não lido, para abrir a janela de Eventos. Para mais informações, por favor consulte em "*Eventos*" (p. 17).

5.4.1. Analisando arquivos e pastas

Pode usar o Dispositivo de Segurança para analisar rapidamente arquivos e pastas. Arraste qualquer arquivo ou pasta que deseje analisar e solte sobre o **Dispositivo Segurança**.

O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção e não podem ser alteradas Caso sejam detectados arquivos infectados, o Bitdefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falhar, o assistente do Analisador Antivírus irá permitir que você especifique outras ações a serem tomadas para os arquivos infectados.

5.4.2. Ocultar/exibir Dispositivo de Segurança

Quando não desejar mais visualizar o dispositivo, clique em .

Para restaurar o Dispositivo Segurança, use um dos seguintes métodos:

- Para a bandeja do sistema:
  1. Clique com o botão direito no ícone do Bitdefender na área de notificação.
  2. Clique em **Exibir Dispositivo Segurança** no menu contextual que aparece.
- A partir da interface do Bitdefender:
  1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
  2. Na janela **Configurações Gerais**, selecione a aba **Configurações Gerais**.
  3. Ligar **Exibir Dispositivo Segurança** clicando no botão correspondente.

5.5. Relatório de Segurança

O Relatório de Segurança fornece um status semanal para seu produto e diversas dicas para melhorar a proteção do sistema. Essas dicas são importantes para gerenciar a proteção geral e você poderá facilmente identificar as ações que pode tomar para seu sistema.

O relatório é gerado uma vez por semana e resume informações relevantes sobre as atividades do produto para que você possa facilmente compreender o que ocorreu durante este período.

A informação oferecida pelo Relatório de Segurança se divide em duas categorias:

- Área de **Proteção** - veja informações relacionadas à proteção do seu sistema.
  - **Arquivos analisados**

    Permite visualizar os arquivos analisados pelo Bitdefender durante a semana. Você pode ver detalhes como o número de arquivos analisados e o número de arquivos limpos pelo Bitdefender.

    Para mais informações sobre a proteção antivirus, por favor consulte "*Proteção Antivírus*" (p. 80).
  - **Páginas Analisadas**

    Permite verificar o número de páginas Web analisadas e bloqueadas pelo Bitdefender. Para o proteger da divulgação de informações pessoais durante a navegação, o Bitdefender protege o seu tráfego na Internet.

    Para mais informações sobre a Proteção da Internet, consulte "*Proteção da Internet*" (p. 115).
  - **Vulnerabilidades**

    Permite identificar e corrigir facilmente as vulnerabilidades do sistema, para tornar o computador mais seguro contra malware e hackers.

    Para mais informações sobre a Análise de Vunerabilidade, por favor consulte a seção "*Vulnerabilidade*" (p. 119).
  - **Linha do Tempo de Eventos**

    Permite que você tenha uma visão geral de todos os processos e problemas reparados pelo Bitdefender durante a semana. Os eventos são separados por dias.

Para mais informações sobre um registro detalhado de eventos relativos à atividade em seu computador, consulte Eventos.

- Área de **Otimização** - veja informações relacionadas ao espaço liberado, aplicativos otimizados e quanta bateria do computador você economizou utilizando o Modo de Bateria.
  - **Bateria economizada**

    Permite que você veja o quanto de bateria você economizou enquanto o sistema funcionou em Modo de Bateria.

    Para mais informações sobre o Modo de Bateria, consulte *"Modo de Bateria"* (p. 21).
  - **Aplicativos otimizados**

    Permite que você veja o número de aplicativos utilizados nos Perfis.

    Para mais informações sobre Perfis, consulte *"Perfis"* (p. 160).

5.5.1. Verificando o Relatório de Segurança

O Relatório de segurança utiliza um sistema de rastreio de problemas para detectar e lheinformar sobre os problemas que podem afetar a segurança do seu computador edados. As incidências detectadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco à segurança. Ao utilizar o relatório, você pode configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger o seu computador e dados privados.

Para verificar o Relatório de segurança, faça o seguinte:

1. Acessar o relatório:
   - Clique no ícone no topo da interface do Bitdefender e então selecione **Relatório de Segurança** na lista de opções.
   - Clique com o botão direito do mouse no ícone do Bitdefender na bandeja do sistema e selecione **Mostrar Relatório de Segurança**.
   - Após a conclusão de um relatório, você receberá uma notificação pop-up. Clique em **Exibir** para acessar ao relatório de segurança.

     Será aberta uma webpage no navegador onde você poderá visualizar o relatório gerado.

2. Observe a parte superior da janela para visualizar o status geral de segurança.
3. Veja as recomendações na parte inferior da página.

A cor da área de status da segurança muda dependendo das incidências detectadas e são apresentadas diferentes mensagens:

- **A área está verde.** Não existem problemas a corrigir. Seu computador e dados estão protegidos.
- **A área está amarela.** A segurança do seu sistema está sendo afetada por problemas não críticos. Deve verificá-las e repará-las quando tiver oportunidade.
- **A área está vermelha.** A segurança do seu sistema está sendo afetada por problemas críticos. Você deve resolver os problemas detectados imediatamente.

5.5.2. Ativar ou desativar a notificação de Relatório de Segurança

Para ligar ou desligar a notificação do Relatório de Segurança, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Configurações Gerais**, selecione a aba **Configurações Gerais**.
3. Clique no botão correspondente para ativar ou desativar a notificação de Relatório de Segurança.

   A notificação do Relatório de Segurança está ativada por padrão.

6. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma virtual onde você tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Você pode acessar sua conta Bitdefender Central de qualquer computador ou dispositivo móvel conectado à Internet visitando https://central.bitdefender.com. Uma vez que você tenha obtido acesso, você pode realizar as seguintes ações:

- Fazer download e instalar o Bitdefender nos sistemas operacionais Windows, OS X e Android. Os produtos disponíveis para download são:
  - Bitdefender Internet Security 2016
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security
- Controlar e renovar suas assinaturas do Bitdefender.
- Adicionar novos dispositivos à sua rede e controlar suas funções de onde quer que você esteja.

6.1. Acessar sua conta Bitdefender Central

Há várias formas de acessar sua conta Bitdefender Central. Dependendo da tarefa que você quiser realizar, você pode utilizar qualquer uma das seguintes opções:

- Na interface principal do Bitdefender:
  1. Clique no link **Ir a Bitdefender Central** na lateral esquerda da interface do Bitdefender.
- Na tela Informações da Conta:
  1. Clique no ícone no topo da interface do Bitdefender e então selecione **Informações da Conta** na lista de opções.
  2. Clique no link **Ir a Bitdefender Central** na parte inferior da janela que abrirá.
- No seu navegador da Internet:
  1. Abrir um navegador em qualquer dispositivo com acesso à Internet.

2. Acesse: https://central.bitdefender.com.
3. Inicie sessão na sua conta com o seu e-mail e senha.

6.2. Minhas assinaturas

A plataforma da Bitdefender Central possibilita que você controle facilmente as assinaturas de todos os seus dispositivos.

6.2.1. Verificar assinaturas disponíveis

Para verificar suas assinaturas disponíveis:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Minhas Assinaturas**.

Aqui você pode acessar informações sobre a disponibilidade das assinaturas que você possui e o número de dispositivos utilizando cada uma delas.

Você pode adicionar um novo dispositivo a uma assinatura ou renová-la selecionando um cartão de assinatura.

Nota
Você pode ter uma ou mais assinaturas em sua conta, desde que sejam para produtos diferentes.

6.2.2. Adicionar novo dispositivo

Caso sua assinatura cubra mais de um dispositivo, você pode adicionar um novo dispositivo e instalar seu Bitdefender Internet Security 2016 nele, como descrito abaixo:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**, e então clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Em outro dispositivo**.

Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

5. Espere o download ser concluído, depois execute o instalador:

6.2.3. Renove assinatura

Caso não tenha escolhido renovar automaticamente sua assinatura do Bitdefender, você pode renová-la manualmente seguindo estas instruções:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Minhas Assinaturas**.
3. Selecione o cartão de assinatura desejado.
4. Clique em **Renovar** para continuar.

Uma página abrirá no seu navegador onde você poderá renovar a sua assinatura do Bitdefender.

6.2.4. Ativar assinatura

Uma assinatura pode ser ativada durante o processo de instalação utilizando sua conta Bitdefender Central. Com o processo de ativação, o período de validade da assinatura começa a contar.

Caso você tenha comprado um código de ativação de um de nossos revendedores ou ganhado como presente, você poderá estender sua assinatura do Bitdefender, desde que o código e sua assinatura sejam do mesmo produto.

Para ativar uma assinatura com um código de ativação, siga os passos abaixo:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Minhas Assinaturas**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e então digite o código no campo correspondente.
4. Clique em **ENVIAR**.

A assinatura está ativada agora. Vá ao painel **Meus dispositivos** e selecione **INSTALAR o Bitdefender** para instalar o produto em um de seus dispositivos.

6.3. Meus dispositivos

A seção **Meus Dispositivos** em sua conta Bitdefender Central permite que você instale, controle e realize ações remotas em seu Bitdefender em qualquer dispositivo, desde que esteja ligado e conectado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado de sua proteção e tempo disponível da assinatura.

Para identificar facilmente seus dispositivos, você pode personalizar o nome de cada dispositivo:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone ⋮ no cartão de dispositivo desejado, e então selecione **Configurações**.
4. Altere o nome do dispositivo no campo correspondente, e então selecione **Salvar**.

Caso o Autopilot esteja desligado, você pode ligá-lo clicando no botão. Clique em **Salvar** para aplicar as configurações.

Você pode criar e atribuir um proprietário a cada um de seus dispositivos para uma melhor gestão:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone ⋮ no cartão de dispositivo desejado, e então selecione **Perfil**.
4. Clique **Adicionar proprietário** e preencha os campos correspondentes. Defina o Sexo, Data de nascimento e selecione até uma Foto de perfil.
5. Clique em **ADICIONAR** para salvar o perfil.
6. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente em um dispositivo, siga os seguintes passos:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.

3. Clique no ícone ⋮ no cartão de dispositivo desejado, e então selecione **Atualizar**.

Para mais ações remotas e informações sobre seu produto Bitdefender em um dispositivo específico, clique no cartão de dispositivo desejado.

Quando você clicar no cartão de dispositivo, as abas a seguir aparecerão:

- **PAINEL**. Nesta janela você pode verificar o estado da proteção dos seus produtos Bitdefender e o número de dias restantes em sua assinatura. O estado da proteção pode estar verde, quando não houver problemas afetando seu dispositivo, ou vermelho quando o dispositivo estiver em risco. Quando houver problemas afetando seu produto, clique em **Visualizar incidências** para descobrir mais detalhes. Daqui você poderá resolver manualmente os problemas que afetam a segurança de seus dispositivos.
- **Proteção**. Desta janela você pode executar uma Verificação Rápida ou do Sistema em seus dispositivos remotamente. Clique no botão **VERIFICAR** para iniciar o processo. Você também pode conferir quando a última verificação foi realizada no dispositivo e acessar um relatório da última verificação, contendo as informações mais importantes.Para mais informações sobre esses dois processos de verificação, acesse “*Executando uma Análise do Sistema*” (p. 88) e “*Executar uma Análise Rápida*” (p. 87).
- **Vulnerabilidade**. Para verificar um dispositivo e identificar vulnerabilidades, como a falta de atualizações do Windows, aplicativos desatualizados ou senhas fracas, clique no botão **VERIFICAR** na aba Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente. Caso alguma seja encontrada, você deve realizar uma nova verificação de vulnerabilidades no dispositivo problemático e então realizar as ações recomendadas. Para mais detalhes sobre esta função, por favor acesse “*Vulnerabilidade*” (p. 119).

7. MANTENDO O SEU BITDEFENDER ATUALIZADO

Novo malware é achado e identificado todos os dias. É por isso que é muito importante manter o Bitdefender atualizado com as últimas assinaturas de malware.

Se você se conectar a Internet através de banda-larga ou DSL, o Bitdefender se encarrega da atualização. Por padrão, o mesmo verifica se há atualizações quando você liga o computador e depois disso, a cada **hora** . Se alguma atualização for detectada, esta será automaticamente baixada e instalada em seu computador.

O processo de actualização é executado em tempo real, o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Importante

Para estar protegido contra as mais recentes ameaças mantenha a Atualização Automática ativada.

Em algumas situações particulares, a sua intervenção é necessária para manter a proteção do Bitdefender atualizada:

- Se o seu computador se conectar à Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de conexão à Internet?*" (p. 73).
- Se não possui uma conexão à Internet, pode atualizar Bitdefender manualmente conforme descrito em "*O meu computador não está conectado à Internet. Como eu posso atualizar o Bitdefender?*" (p. 178). O arquivo de atualização manual é liberado uma vez por semana.
- Podem ocorrer erros ao baixar atualizações com uma conexão lenta à Internet. Para saber como superar tais erros, consulte "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 177).
- Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o Bitdefender a pedido do usuário. Para mais informações, por favor consulte "*Efetuar uma atualização*" (p. 44).

7.1. Verifique se o Bitdefender está atualizado

Para verificar a data da última atualização de seu Bitdefender, observe a **Área do Status de Segurança**, do lado esquerdo da barra de ferramentas.

Para informações mais detalhadas sobre as mais recentes atualizações, verifique os eventos de atualização:

1. Na janela principal, clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Atualizar** no menu suspenso correspondente.

Você pode saber quando foram iniciadas as atualizações e obter informações sobre as mesmas (se foram bem sucedidas ou não, se é necessário reiniciar para concluir a instalação). Se necessário, reinicie o sistema quando lhe convier.

7.2. Efetuar uma atualização

Para realizar atualizações, é necessária uma conexão à Internet.

Para iniciar uma atualização, faça o seguinte:

- Abra a interface do Bitdefender e clique no botão de ação **Atualizar**.
- Clique com o botão direito no ícone do Bitdefender na barra de sistema e selecione **Atualizar Agora**.

O módulo Atualização irá conectar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações. Se uma atualização é detectada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das configurações de atualização.

Importante

Talvez seja necessário reiniciar o computador depois da atualização. Nós recomendamos que você o faça o mais rápido possível.

Você também pode realizar atualizações remotamente em seus dispositivos, desde que estejam ligados e conectados à Internet.

Para atualizar o Bitdefender remotamente em um dispositivo, siga os seguintes passos:

1. Acesse sua conta Bitdefender Central.

2. Selecione o painel **Meus Dispositivos**.

3. Clique no ícone ⋮ no cartão de dispositivo desejado, e então selecione **Atualizar**.

7.3. Ligar ou desligar a atualização automática

Para ativar ou desativar a análise automática, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela de **Configurações Gerais**, selecione a aba **Atualizar**.
3. Clique no botão para ativar ou desativar a atualização automática.
4. Uma janela de alerta aparece. Você deve confirmar a sua escolha selecionando no menu por quanto tempo deseja desativar a atualização automática. Você pode desativar as atualizações automáticas por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desative a atualização automática pelo menor tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de proteger você contra as ameaças mais recentes.

7.4. Ajuste das configurações de atualização

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy. Por padrão, o Bitdefender verificará as atualizações de hora em hora, via Internet, e instalará as que estejam disponíveis sem alertar você.

As configurações de atualização padrão são adequadas à maioria dos usuários e normalmente não precisam ser alteradas.

Para ajustar as definições de atualização, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.

2. Na janela **Configurações Gerais**, selecione a aba **Atualizar** e ajuste as configurações de acordo com suas preferências.

Frequência de atualização

O Bitdefender está configurado para procurar atualizações a cada hora. Para alterar a frequência de atualização, arraste o marcador pela barra de frequência para definir o intervalo em que as atualizações devem ocorrer.

Local de atualização

Bitdefender está configurado para ser atualizado a partir dos servidores de atualização de Bitdefender na Internet. A localização de atualização é um endereço genérico da Internet que é automaticamente redirecionado para o servidor de atualização da Bitdefender mais próximo da sua região.

Não altere a localização da atualização exceto se tiver sido aconselhado por um representante da Bitdefender ou pelo administrador da sua rede (se estiver conectado a uma rede no escritório).

Pode voltar à localização de atualização genérica da Internet clicando em **Predefinição**.

Regras de processamento da atualização

Pode escolher entre três formas para baixar e instalar atualizações:

- **Atualização Silenciosa** - O Bitdefender faz download automaticamente e implementa a atualização.
- **Consultar antes do download** - sempre que uma atualiação estiver disponível, você será consultado antes do download ser efetuado.
- **Avisar antes de instalar** - cada vez que uma atualização for baixada, você será consultado antes da instalação ser feita.

Algumas atualizações exigem o reinício para concluir a instalação. Por padrão, se for necessário reiniciar após uma atualização, o Bitdefender continuará a trabalhar com os arquivos antigos até que o usuário reinicie voluntariamente o computador. Isto serve para evitar que o processo de atualização de Bitdefender interfira com o trabalho do usuário.

Se quiser ser avisado quando uma atualização exigir uma reinicialização, desligue a opção **Adiar reiniciar** clicando no botão correspondente.

COMO

8. INSTALAÇÃO

8.1. Como instalo o Bitdefender num segundo computador?

Caso a assinatura que você comprou cubra mais de um computador, você pode utilizar sua conta Bitdefender Central para registrar um segundo PC.

Para instalar o Bitdefender em um segundo computador, siga estes passos:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo.**

     Na lista **Produto a ser instalado**, selecione o Bitdefender Internet Security 2016 e então clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Em outro dispositivo.**

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Execute o Bitdefender que você baixou. Aguarde até que o processo de instalação esteja concluído e feche a janela.

O novo dispositivo em que você instalou o Bitdefender aparecerá no painel de controle da Bitdefender Central.

8.2. Quando devo reinstalar o Bitdefender?

Em algumas situações poderá ser necessário reinstalar o seu produto Bitdefender.

As situações típicas em que deve reinstalar Bitdefender são as seguintes:

- você reinstalou o sistema operacional.
- adquiriu um computador novo.
- deseja alterar a língua da interface do Bitdefender.

Para reinstalar o Bitdefender, você pode utilizar o disco de instalação que você comprou ou baixar uma nova versão na sua conta Bitdefender Central.

Para mais informações sobre o processo de instalação do Bitdefender, por favor consulte o "*Instalando seu produto Bitdefender*" (p. 5).

8.3. Onde posso baixar meu produto Bitdefender?

Você pode instalar o Bitdefender do disco de instalação, ou utilizando o instalador baixado na plataforma Bitdefender Central.

Nota

Antes de executar o kit é recomendável remover qualquer solução antivírus instalada no seu sistema. Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.

Para instalar o Bitdefender da conta Bitdefender Central, siga estes passos:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**, e então clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Em outro dispositivo**.

     Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Execute o Bitdefender que você baixou.

8.4. Como utilizar minha assinatura do Bitdefender após uma atualização do Windows?

Esta situação ocorre quando você atualiza seu sistema operacional e deseja continuar utilizando sua assinatura do Bitdefender.

Se você estiver usando uma versão anterior do Bitdefender, você pode atualizar, gratuitamente para a versão mais recente do Bitdefender, da seguinte forma:

- Da versão anterior do Bitdefender Antivirus para a versão mais recente doBitdefender Antivirus.
- Da versão anterior do Bitdefender Internet Security para a versão mais recente do Bitdefender Internet Security.
- Da versão anterior do Bitdefender Total Security para a versão mais recente do Bitdefender Total Security.

Há duas possibilidades de caso que podem aparecer:

- Você atualizou o sistema operacional utilizando o Windows Update e você percebe que o Bitdefender não está mais funcionando.

  Neste caso, será necessário reinstalar o produto usando a versão mais recente disponível.

  Para resolver esta situação, siga os seguintes passos:

  1. Remova o Bitdefender seguindo estes passos:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
       d. Clique em **Próximo** para continuar.
       e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
     - No **Windows 8 e Windows 8.1**:
       a. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
d. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
e. Clique em **Próximo** para continuar.
f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 10**:
  a. Clique em **Iniciar** e depois em Configurações.
  b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
  d. Clique em **Desinstalar** novamente para confirmar sua escolha.
  e. Clique em **Remover** na janela que se abrirá. Logo, selecione **Quero reinstalá-lo**.
  f. Clique em **Próximo** para continuar.
  g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

2. Baixe o arquivo de instalação:
   a. Acesse sua conta Bitdefender Central.
   b. Selecione o painel **Meus Dispositivos**.
   c. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
   d. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
      - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

        Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**, e então clique em **Download** para continuar.
      - Eu gostaria de instalar o Bitdefender **Em outro dispositivo**.

        Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

3. Localize e dê um clique duplo no instalador para iniciar o processo de instalação.

- Você mudou seu sistema e deseja continuar usando a proteção Bitdefender.

  Portanto, será necessário reinstalar o produto usando a versão mais recente.

  Para resolver este problema:

  1. Baixe o arquivo de instalação:
     a. Acesse sua conta Bitdefender Central.
     b. Selecione o painel **Meus Dispositivos**.
     c. Na janela **Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
     d. Escolha **Windows**, depois escolha uma das duas opções disponíveis:
        - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

          Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**, e então clique em **Download** para continuar.
        - Eu gostaria de instalar o Bitdefender **Em outro dispositivo**.

          Selecione o Bitdefender Internet Security 2016 da lista **Produto a ser instalado**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
  2. Localize e dê um clique duplo no instalador para iniciar o processo de instalação.

  Para mais informações sobre o processo de instalação do Bitdefender, por favor consulte o “*Instalando seu produto Bitdefender*” (p. 5).

8.5. Como posso reparar o Bitdefender?

Caso queira reparar seu Bitdefender Internet Security 2016 a partir do menu Iniciar do Windows, siga estes passos:

- No **Windows 7**:
  1. Clique **Iniciar** e acesse **Todos os Programas**.
  2. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
  3. Clique em **Reparar** na janela que aparece.

Isto irá demorar vários minutos.

4. Precisará de reiniciar o computador para concluir o processo

- No **Windows 8 e Windows 8.1**:
  1. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Reparar** na janela que aparece.

     Isto irá demorar vários minutos.
  5. Precisará de reiniciar o computador para concluir o processo
- No **Windows 10**:
  1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos e recursos**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Clique em **Reparar**.

     Isto irá demorar vários minutos.
  6. Precisará de reiniciar o computador para concluir o processo

9. ASSINATURAS

9.1. Que produto Bitdefender estou usando?

Para descobrir que programa do Bitdefender você instalou:

1. Abra a interface do Bitdefender.
2. Na parte superior da janela você verá o seguinte:
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. Como ativo minha assinatura do Bitdefender utilizando um botão de licença?

Se você tem uma chave de licença e deseja utilizá-la para ativar uma assinatura do Bitdefender Internet Security 2016, há dois possíveis casos que podem ser aplicáveis:

- Você atualizou uma versão anterior do Bitdefender para a mais recente:
  1. Uma vez que a atualização para o Bitdefender Internet Security 2016 estiver completa, será solicitado que você acesse sua conta Bitdefender Central.
  2. Digite suas credenciais de acesso e clique em **ENTRAR**
  3. Uma notificação informando que uma assinatura foi criada aparecerá na tela da sua conta. A assinatura criada será válida pelo número de dias restantes em sua chave de licença e para o mesmo número de usuários.

     Dispositivos que utilizem versões anteriores do Bitdefender que estiverem registradas com a chave de licença que você converteu a uma assinatura precisam registrar o produto na mesma conta Bitdefender Central.
- O Bitdefender não foi instalado anteriormente no sistema:
  1. Assim que o processo de instalação estiver completo, será solicitado que você acesse sua conta Bitdefender Central.

2. Digite suas credenciais de acesso e clique em **ENTRAR**
3. Selecione o painel **Minhas Assinaturas**.
4. Clique no botão **Adicionar chave de licença** e digite sua chave de licença.
5. Uma assinatura com a mesma validade e número de usuários de sua chave de licença está associada à sua conta.

10. BITDEFENDER CENTRAL

10.1. Como acesso Bitdefender Central utilizando outra conta online?

Você criou uma nova conta Bitdefender Central e deseja utilizá-la de agora em diante.

Para usar outra conta com sucesso, siga estes passos:

1. Clique no ícone no topo da interface do Bitdefender e selecione **Informações da conta** na lista de opções.
2. Clique no botão **Alterar conta** para trocar a conta vinculada ao computador.
3. Digite o endereço de e-mail e a senha da sua conta nos campos correspondentes, e então clique em **ENTRAR**.

Nota
O produto Bitdefender em seu dispositivo muda automaticamente de acordo com a assinatura associada à nova conta Bitdefender Central.
Se não houver uma assinatura associada à nova conta Bitdefender Central, ou caso você deseje transferi-la da conta anterior, você pode contatar o Bitdefender para obter suporte, como descrito na seção *"Solicite Ajuda"* (p. 201).

10.2. Como posso redefinir minha senha para a conta Bitdefender Central?

Para definir uma nova senha para sua conta Bitdefender Central, siga estes passos:

1. Clique no ícone no topo da interface do Bitdefender e selecione **Informações da conta** na lista de opções.
2. Clique no botão **Alterar conta** para trocar a conta vinculada ao computador.

   Uma nova janela aparece.
3. Clique no link **Redefinir senha**.
4. Digite o endereço de e-mail utilizado para criar sua conta Bitdefender Central, e então clique no botão **REDEFINIR SENHA**.

5. Verifique seu e-mail e clique no link fornecido.
6. Digite seu endereço de e-mail no campo correspondente.
7. Digite a nova senha. A senha deve possuir no mínimo 8 caracteres e incluir números.
8. Clique em **DEFINIR SENHA**.

Para acessar sua conta Bitdefender Central daqui em diante, digite seu endereço de e-mail e a senha que você acabou de definir.

11. A ANALISAR COM BITDEFENDER

11.1. Como posso analisar um arquivo ou uma pasta?

A forma mais fácil para analisar um arquivo ou pasta é clicar com o botão direito no objeto que deseja analisar, apontar para o Bitdefender e selecionar **Analisar com o Bitdefender** a partir do menu.

Para concluir a análise, siga o assistente de Análise Antivírus. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.

Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

Situações típicas da maneira que você pode utilizar esse método de análise:

- Você suspeita que um arquivo específico ou diretório esteja infectado.
- Sempre que você faz download de arquivos da Internet e suspeita que podem ser perigosos.
- Analisar um compartilhamento de rede antes de copiar os arquivos para o computador.

11.2. Como posso analisar o meu sistema?

Para realizar uma análise completa ao sistema, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise de Sistema**.
4. Siga as instruções do assistente de Verificação de Sistema para completar a verificação. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.

   Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas. Para mais informações, por favor consulte *"Assistente do analisador Antivírus"* (p. 92).

11.3. Como programar uma verificação?

Você pode configurar seu produto Bitdefender para iniciar a verificação de locais importantes do sistema quando você não estiver utilizando o computador.

Para programar uma verificação, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Gerenciar Verificações**.
4. Escolha o tipo de verificação que deseja realizar, Verificação de Sistema ou Verificação Rápida, e então clique em **Opções de verificação**.

   Você também pode criar um tipo de verificação que atenda às suas necessidades clicando em **Nova tarefa personalizada**.
5. Ativar o botão **Programar**.

   Escolha uma das opções correspondentes para definir uma agenda:
   - No início do sistema
   - Uma vez
   - Periodicamente

Na janela **Verificar metas**, você pode selecionar os locais que você deseja verificar.

11.4. Como posso criar uma tarefa de análise personalizada?

Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.

Para criar uma tarefa de análise personalizada, proceda da seguinte forma:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Gerenciar Verificações**.

4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem escaneadas.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**.

   Você pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido.

   Também pode optar por desligar o computador sempre que a análise termina, se não forem encontradas ameaças. Lembre-se de que esta será a ação padrão sempre que executar esta tarefa.
6. Clique em **OK** para guardar as alterações e fechar a janela.
7. Utilize o botão correspondente se você deseja definir um agendamento para a sua tarefa de verificação.
8. Clique em **Iniciar verificação** e siga as instruções do assistente de verificação para completar a verificação. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.
9. Se quiser, você pode refazer rapidamente a verificação customizada anterior ao clicar na entrada correspondente na lista.

11.5. Como posso excluir uma pasta da análise?

O Bitdefender permite excluir arquivos, pastas ou extensões de arquivos específicos da análise.

As exceções devem ser usadas pelos usuários que possuem conhecimentos avançados em informática e apenas nas seguintes situações:

- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um arquivo grande no seu sistema onde guarda diferentes dados.
- Você mantém uma pasta onde instalar diferentes tipos de software e aplicativos para testes. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar a pasta à lista de Exceções, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.

2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Exclusões**
4. Assegure-se de que as **Exclusões de Arquivos** esteja ligada ao clicar no botão.
5. Clique no link **Arquivos e pastas excluídos**.
6. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
7. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**.
8. Clique em **Adicionar** e depois em **OK** para salvar as alterações e fechar a janela.

11.6. O que fazer se o Bitdefender identificou um arquivo limpo como infectado?

Pode haver casos em que o Bitdefender assinala erradamente um arquivo legítimo como sendo uma ameaça (um falso positivo). Para corrigir este erro, adicione o arquivo à área de Exclusões do Bitdefender:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone no canto inferior direito da interface do Bitdefender.
   b. Selecione a aba **Proteção**.
   c. Clique no módulo **Antivírus**.
   d. Na janela **Antivírus**, selecione a aba **Shield**.
   e. Clique no botão para desligar **Análise no-acesso**.

      Uma janela de alerta aparece. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a proteção em tempo real. Você pode desativar a proteção em tempo real por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema.
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte *"Como posso mostrar objetos ocultos no Windows?"* (p. 75).
3. Restaurar o arquivo da área de Quarentena:

a. Clique no ícone no canto inferior direito da interface do Bitdefender.
b. Selecione a aba **Proteção**.
c. Clique no módulo **Antivírus**, depois selecione a aba **Quarentena**
d. Selecione um arquivo e clique em **Restaurar**.

4. Adicionar o arquivo à lista de Exceções. Para saber como fazer isto, consulte “*Como posso excluir uma pasta da análise?*” (p. 60).
5. Active a proteção antivírus em tempo real do Bitdefender.
6. Contate os nossos representantes do suporte para que possamos remover a assinatura de detecção. Para saber como fazer isto, consulte “*Solicite Ajuda*” (p. 201).

11.7. Como posso verificar quais vírus o Bitdefender detectou?

Cada vez que uma análise é realizada, um registro de análise é criado e o Bitdefender registra as incidências detectadas.

O relatório da análise contém informação detalhada sobre os processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

Pode abrir o relatório directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar um relatório de análise ou qualquer infecção detectada posteriormente, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** no menu suspenso correspondente.

   Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo usuário e alterações de status para as análises automáticas.
3. Na lista de eventos, pode ver as análises que foram recentemente efetuadas. Clique no evento para visualizar detalhes sobre o mesmo.
4. Para abrir um relatório da análise, clique em **Visualizar Relatório**.

Caso você deseje realizar a mesma verificação novamente, clique no botão **Verificar novamente**.

12. CONSULTOR PARENTAL

12.1. Como posso proteger os meus filhos de ameaças online?

O Consultor Parental do Bitdefender permite que você restrinja acesso à Internet e a aplicativos específicos, prevenindo que seus filhos visualizem conteúdos inapropriados quando você não estiver por perto.

Para configurar o Consultor Parental, siga estes passos:

1. Criar uma conta do Windows limitada (standard) para a sua criança usar. Para mais informações, por favor consulte *"Como posso criar contas de usuário do Windows?"* (p. 68).
2. Certifique-se que tem a sessão iniciada com a conta de administrador. Somente usuários com privilégios administrativos no sistema (administradores) podem acessar e configurar o Consultor Parental.
3. Configure o Consultor Parental para as contas de usuário do Windows que seu filho utilizar.

   a. Clique no ícone no canto inferior direito da interface do Bitdefender.

   b. Selecione a aba **Privacidade**.

   c. No módulo **Consultor Parental**, selecione **Configurar**.

   Você será redirecionado à página da Bitdefender Central. Assegure-se de acessar a conta com suas creden

   d. O painel de controle do Consultor Parental abrirá em uma nova janela. Aqui você poderá checar e alterar as configurações do Consultor Parental.

   e. Clique em **ADICIONAR PERFIL** na lateral direita da janela **Meus filhos**.

   f. Preencha os campos com informações específicas, como: nome, e-mail, sexo e data de nascimento, e então clique em **CONTINUAR**.

   Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as especificações consideradas apropriadas para sua faixa etária.

g. Caso o dispositivo de seu filho já possua o Bitdefender Internet Security 2016 instalado, selecione esse dispositivo da lista disponível e clique em **CONTINUAR**.

   Caso o dispositivo de seu filho não tenha nenhum Bitdefender com a função de Consultor Parental incluído, clique em **Adicionar novo dispositivo**. Selecione o sistema operacional desse dispositivo e clique em **CONTINUAR**.

   Digite o endereço de e-mail para onde devemos enviar o link de download de instalação do aplicativo Consultor Parental do Bitdefender.

   Em dispositivos com Windows, o Bitdefender Internet Security 2016 que você incluiu em sua assinatura deverá ser baixado e instalado. Em dispositivos Android, o Agente Consultor Parental do Bitdefender deverá ser baixado e instalado.

Verifique as atividades de seus filhos e altere as configurações do Consultor Parental utilizando a Bitdefender Central desde qualquer computador ou dispositivo móvel conectado à Internet.

12.2. Como bloqueio o acesso do meu filho a um website?

O Consultor Parental do Bitdefender permite que você controle o conteúdo acessado por seus filhos em seus dispositivos, e permite que você bloqueie acesso a determinados sites.

Para bloquear o acesso a um sítio, você precisa adicioná-lo à lista de Exceções, como abaixo:

1. Acesse: https://central.bitdefender.com.
2. Inicie sessão na sua conta com o seu e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil de seu filho na janela **Meus filhos**.
5. Selecione a aba **Interesses**.
6. Clique no botão **GERENCIAR**.
7. Digite o endereço da página que deseja bloquear no campo correspondente.
8. Selecione **Permitir** ou **Negar**.

9. Clique em **Ok** para salvar as alterações.

12.3. Como impeço o meu filho de jogar um jogo?

O Consultor Parental do Bitdefender permite que você controle o conteúdo acessado por seus filhos enquanto utilizam o computador.

Para bloquear o acesso a um jogo, siga os seguintes passos:

1. Acesse: https://central.bitdefender.com.
2. Inicie sessão na sua conta com o seu e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil de seu filho na janela Meus filhos.
5. Selecione a aba **Atividades**.

   Uma lista com cartões será exibida. Os cartões representam os aplicativos que seu filho utiliza.
6. Selecione o cartão com o aplicativo que você deseja que seu filho pare de utilizar.

   O símbolo de marcação que aparecerá indica que seu filho não poderá utilizar o aplicativo.

12.4. Como previno que meus filhos entrem em contato com pessoas não confiáveis?

O Consultor Parental do Bitdefender possibilita que você bloqueie ligações de números desconhecidos ou de amigos na lista de contatos de seu filho.

Para bloquear um contato específico, siga estes passos:

1. Acesse: https://central.bitdefender.com.

   Assegure-se de acessar a conta com suas creden
2. Clique em **Consultor Parental** para acessar o painel de controle.
3. Clique no ícone ⋮ no cartão de perfil desejado, e então selecione **Editar**.
4. Digite o número de telefone de seu filho no campo correspondente, e então clique em **SALVAR**.
5. Selecione o perfil da criança para qual deseja estabelecer restrições.

6. Selecione a aba **Amigos**.

   Uma lista com cartões será exibida. Os cartões representam os contatos do telefone de seu filho.

7. Selecione o cartão com o número de telefone que você deseja bloquear.

   O símbolo de marcação que aparecerá indica que seu filho não receberá ligações do número de telefone selecionado.

Para bloquear números desconhecidos, ative a opção **nenhuma interação de identificação de chamadas**.

12.5. Como posso definir um local como seguro ou restrito para meu filho?

O Consultor Parental do Bitdefender permite que você defina um local como seguro ou restrito para seu filho.

Para definir um local, siga estes passos:

1. Acesse: https://central.bitdefender.com.

   Assegure-se de acessar a conta com suas creden

2. Clique em **Consultor Parental** para acessar o painel de controle.
3. Selecione o perfil de seu filho na janela **Meus filhos**.
4. Selecione a aba **Lugares**.
5. Clique em **Dispositivos** na janela **Lugares**.
6. Clique em **ESCOLHER DISPOSITIVOS** e então selecione o dispositivo que você deseja configurar.
7. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
8. Escolha o tipo de local, **Seguro** ou **Restrito**.
9. Digite um nome válido para a área onde seu filho tem ou não permissão para ir.
10. Em **Lugar original**, digite a cidade onde seu filho deve estar e escolha o bairro da lista que aparecerá.
11. Defina a distância que deverá ser utilizada para monitoramento na barra **Raio**.
12. Clique em **ADICIONAR ÁREA** para salvar suas configurações.

Sempre que você quiser marcar uma região restrita como segura, ou uma segura como restrita, clique nela e clique no botão **EDITAR ÁREA**. Dependendo da mudança que você deseja realizar, selecione a opção **SEGURO** ou **RESTRITO**, e clique em **ATUALIZAR ÁREA**.

12.6. Como posso criar contas de usuário do Windows?

Uma conta de utilizador do Windows é um perfil exclusivo que inclui todas as definições, os privilégios e os arquivos pessoais de cada utilizador. As contas do Windows permitem ao administrador do PC controlar o acesso dos restantes utilizadores.

É muito útil definir contas de utilizador quando o computador é utilizado tanto por adultos como por crianças - um pai pode definir uma conta para cada filho.

Escolha o seu sistema operativo para saber como criar contas do Windows.

- **Windows 7:**
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar, Painel de Controle e, depois, em Contas de Utilizador.
  3. Clique em Criar uma nova conta.
  4. Escreva o nome do usuário. Você pode utilizar o nome completo, o primeiro nome ou um apelido. Depois, clique em Seguinte.
  5. Para o tipo de conta, clique em Padrão e, depois, em Criar Conta. As contas limitadas são adequadas para crianças pois não permitem alterações ao sistema ou instalação de certos aplicativos.
  6. A sua nova conta será criada e apresentada no ecrã Gerir Contas.
- **Windows 8 e Windows 8.1:**
  1. Inicie sessão no seu computador como administrador.
  2. Aponte o mouse para o canto superior direito da tela, clique em Configurações e então clique em Alterar Configurações do PC.
  3. Clique em Usuários no menu ao lado esquerdo e então clique em Adicionar um usuário.

     Você pode criar uma conta Microsoft ou uma conta Local. Leia a descrição de cada tipo de conta e siga as instruções na tela para criar uma nova conta.

- **Windows 10**:
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar e depois em Configurações.
  3. Selecione Contas, depois Família e outros.
  4. Clique em Adicionar novo usuário neste computador.
  5. Você pode criar uma conta Microsoft ou uma conta Local. Leia a descrição de cada tipo de conta e siga as instruções na tela para criar uma nova conta.

Nota

Agira que adicionou novas contas de utilizador, pode criar senhas para as contas.

12.7. Como remover um perfil de criança

Caso queira remover um perfil de criança existente, siga estes passos:

1. Acesse: https://central.bitdefender.com.
2. Inicie sessão na sua conta com o seu e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Clique no ícone ⋮ no perfil da criança que você deseja apagar, e então selecione **Remover**.

13. PRIVACIDADE

13.1. Como posso ter a certeza de que a minha transação online é segura?

Para ter a certeza de que as suas operações online se mantém privadas, você pode usar o browser fornecido pelo Bitdefender para proteger as suas transações e as suas aplicações bancárias.

O Bitdefender Safepay™ é um navegador projetado para proteger a informação do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que você possa utilizar enquanto acessa diferentes locais on-line.

Para manter a sua atividade online segura e privada, faça o seguinte:

1. Clique no botão de ação **Safepay** na interface do Bitdefender.
2. Clique no ícone para acessar o **Teclado Virtual**.
3. Use o **Teclado Virtual** ao digitar informações delicadas como senhas.

13.2. Como removo um arquivo permanentemente com o Bitdefender?

Caso deseje remover um arquivo permanentemente do seu sistema, é necessário apagar a informação fisicamente do seu disco rígido.

O Destruidor de Arquivos do Bitdefender pode ajudá-lo a rapidamente destruir arquivos ou pastas do seu computador usando o menu contextual do Windows, seguindo os seguintes passos:

1. Clique com o botão direito do mouse no arquivo ou pasta que deseja apagar permanentemente, aponte para o Bitdefender e selecione **Destruidor de Arquivos**.
2. Uma janela de confirmação aparecerá. Clique em **Sim** para iniciar o assistente do Destruidor de Arquivos.
3. Aguarde que o Bitdefender termine a destruição dos arquivos.
4. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

14. INFORMAÇÕES ÚTEIS

14.1. Como testo minha solução antivírus?

Assegure-se que seu produto Bitdefender esteja sendo executado adequadamente, recomendamos utilizar o teste Eicar.

O teste Eicar permite que você verifique sua proteção antivírus utilizando um arquivo de segurança desenvolvido para este propósito.

Para testar sua solução antivírus, siga estes passos:

1. Baixe o teste da página web oficial da organização EICAR http://www.eicar.org/.
2. Clique na aba **Arquivo de Teste Anti-Malware**.
3. Clique em **Baixar** no menu do lado esquerdo.
4. A partir da **area de download utilizando o protocolo padrão http** clique no arquivo de teste **eicar.com**.
5. Você será informado que a página que está tentando acessar contém o Arquivo de Teste EICAR (não é um vírus).

   Caso clique em **Compreendo os riscos, leve-me até lá assim mesmo**, o download do teste irá iniciar e um pop-up do Bitdefender irá informá-lo que um vírus foi detectado.

   Clique em **Maiores Detalhes** para obter maiores informações sobre esta ação.

Caso não receba nenhum alerta de Bitdefender, recomendamos que entre em contato com Bitdefender para suporte conforme descrito na seção “*Solicite Ajuda*” (p. 201).

14.2. Como eu posso remover o Bitdefender?

Caso deseje remover seu Bitdefender Internet Security 2016, siga os seguintes passos:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.

3. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo**.
4. Clique em **Próximo** para continuar.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 8 e Windows 8.1**:
  1. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo**.
  5. Clique em **Próximo** para continuar.
  6. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
  1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo**.
  6. Clique em **Próximo** para continuar.
  7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

14.3. Como desligo automaticamente o meu computador após a análise?

O Bitdefender oferece múltiplas tarefas de análise que você pode usar para se certificar que o seu sistema não está infectado com malware. Analisar todo o computador pode levar muito mais tempo dependendo do hardware do seu sistema e da configuração do seu software.

Por este motivo, o Bitdefender permite configurar o Bitdefender para desligar o computador assim que a análise terminar.

Por exemplo: você terminou de trabalhar no seu computador e deseja ir dormir. Gostaria de ter o seu sistema completamente analisado em busca de malware pelo Bitdefender.

Eis como você deve configurar Bitdefender para desligar o seu computador ao término da análise:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Gerenciar Verificações**.
4. Na janela **Gerenciar tarefas de verificação**, clique em **Nova tarefa personalizada** para definir um nome para a verificação e selecionar os locais a serem verificados.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**.
6. Opte por desligar o computador sempre que a análise terminar e se não forem encontradas ameaças.
7. Clique em **OK** para guardar as alterações e fechar a janela.
8. Clique no botão **Iniciar verificação** para verificar seu sistema.

Se não forem encontradas ameaças, o computador irá desligar.

Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas. Para mais informações, por favor consulte *"Assistente do analisador Antivírus"* (p. 92).

14.4. Como posso configurar Bitdefender para usar um proxy de conexão à Internet?

Se o seu computador se conecta à Internet através de um servidor proxy, você deve configurar as definições de proxy do Bitdefender. Normalmente, o Bitdefender detecta e importa automaticamente as definições proxy do seu sistema.

Importante

As ligações à internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da conexão proxy do seu programa Bitdefender quando as atualizações não funcionarem. Se o Bitdefender atualizar, ele está devidamente configurado para se conectar à Internet.

Para gerenciar as configurações de proxy, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a aba **Avançado**.
3. Ative ou desative a utilização de Proxy clicando no botão.
4. Clique no link **Gerenciar proxies.**
5. Existem duas opções para definir as configurações de proxy:
   - **Importar configurações de proxy do navegador padrão** - configurações de proxy do usuário atual, extraídas do navegador padrão. Caso o servidor proxy exija um nome de usuário e uma senha, você deverá inseri-los nos campos correspondentes.

     Nota

     O Bitdefender pode importar as definições de proxy dos navegadores mais populares, incluindo as versões mais recentes de Internet Explorer, Mozilla Firefox e Opera.

   - **Definições de proxy personalizadas** - definições de proxy que você pode configurar. As seguintes definições devem ser especificadas:
     - **Endereço** - introduza o IP do servidor proxy.
     - **Porta** - insira a porta que o Bitdefender usa para se ligar ao servidor proxy.
     - **Usuário do proxy** - digite um usuário reconhecido pelo Proxy.
     - **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.
6. Clique em **OK** para guardar as alterações e fechar a janela.

O Bitdefender usará as configurações de proxy disponíveis até conseguir conexão à Internet.

14.5. Estou usando uma versão de 32 ou 64 Bit do Windows?

Para saber se tem um sistema operativo de 32 bit ou 64 bit, siga os seguintes passos:

- No **Windows 7**:
  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e selecione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.
- No **Windows 8 e Windows 8.1**:
  1. A partir da tela Iniciar do Windows, localize **Computador** (por exemplo, você pode começar a digitar "Computador" diretamente no menu Iniciar) e então clicar com o botão direito do mouse em seu ícone.
  2. Selecione **Propriedades** no menu inferior.
  3. Veja o tipo do seu sistema na área do Sistema.
- No **Windows 10**:
  1. Digite "Sistema" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente.
  2. Procure por informações sobre o tipo do sistema na área do Sistema.

14.6. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de malware e tiver de encontrar e remover os arquivos infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, acesse **Painel de Controle**.

   No **Windows 8 e Windows 8.1**: Na tela Iniciar do Windows, localize o **Painel de Controle** (por exemplo, digite "Painel de Controle" na tela Iniciar) e clique no ícone com o botão direito.
2. Selecione **Opções de Pasta**.
3. Acesse a aba **Visualizar**.

4. Selecione **Mostrar arquivos e pastas ocultos**.
5. Desmarque **Ocultar extensões nos tipos de arquivo conhecidos**.
6. Desmarque **Ocultar arquivos protegidos do sistema operativo**.
7. Clique em **Aplicar**, depois em **OK**.

No **Windows 10**:

1. Digite "Mostrar arquivos e pastas ocultos" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente.
2. Selecione **Mostrar arquivos, pastas e diretórios ocultos**.
3. Desmarque **Ocultar extensões nos tipos de arquivo conhecidos**.
4. Desmarque **Ocultar arquivos protegidos do sistema operativo**.
5. Clique em **Aplicar**, depois em **OK**.

14.7. Como posso remover outras soluções de segurança?

A principal razão para utilizar uma solução de segurança é proporcionar proteção e segurança aos seus dados. Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável. O instalador do Bitdefender Internet Security 2016 detecta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial, siga os seguintes passos:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 8 e Windows 8.1**:
  1. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  4. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
  1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do sítio de Internet do fornecedor ou contacte-o directamente para receber instruções de desinstalação.

14.8. Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detectar e resolver problemas que estejam a afectar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a vírus que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria dos vírus está inactiva quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

1. Reinicie o computador.
2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para acessar ao menu de arranque.
3. Selecione **Modo Seguro** no menu de inicialização ou **Modo Seguro com Rede** se quiser ter acesso à Internet.
4. Pressione **Enter** e aguarde enquanto o Windows carrega em Modo de Segurança.
5. Este processo termina com uma mensagem de confirmação. Clique em **OK** para aceitar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

GERENCIAR A SUA SEGURANÇA

15. PROTEÇÃO ANTIVÍRUS

Bitdefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora). A proteção que o Bitdefender oferece está dividida em duas categorias:

- Análise no acesso - previne que novas ameaças de malware entrem no seu sistema. Por exemplo, Bitdefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

  A análise no acesso garante proteção em tempo real contra malware, sendo um componente essencial de qualquer programa de segurança de computador.

  Importante
  Para prevenir que o seu computador seja infectado por vírus, mantenha ativada a **análise no acesso**.

- Análise a-pedido - permite detectar e remover malware que já se encontra a residir no seu sistema. Esta é uma análise clássica iniciada pelo usuário – você escolhe qual a drive, pasta ou arquivo o Bitdefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer mídia removível que esteja conectada ao computador para garantir um acesso seguro. Para mais informações, por favor consulte “*Análise automática de mídia removível*” (p. 96).

Os utilizadores avançados podem configurar as exclusões da análise se não quiserem que certos arquivos ou tipos de arquivos sejam analisados. Para mais informações, por favor consulte “*Configurar exceções da análise*” (p. 98).

Quando detecta um vírus ou outro malware, o Bitdefender irá tentar remover automaticamente o código de malware do arquivo e reconstruir o arquivo original. Esta operação é designada por desinfecção. Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informações, por favor consulte “*Gerenciar arquivos em quarentena*” (p. 100).

Se o seu computador estiver infectado com malware, por favor consulte “*Remover malware do seu sistema*” (p. 191). Para ajudá-lo a remover o malware

do computador que não pode ser removido no sistema operacional Windows, o Bitdefender lhe fornece o Modo de Recuperação. Este é um ambiente confiável especialmente concebido para a remoção de malware, o que lhe permite inicializar o computador independentemente do Windows. Quando o computador estiver sendo executado no Modo de Recuperação, o malware do Windows fica inativo, tornando-se mais fácil a sua remoção.

Para proteger seu computador de aplicativos maliciosos, o Bitdefender usa o Controle Ativo de Ameaças, uma tecnologia heurística avançada que monitora continuamente os aplicativos em execução no sistema. O Controle Ativo de Ameaças bloqueia automaticamente aplicativos que exibam comportamentos semelhantes a malwares para impedir que danifiquem seu computador. Ocasionalmente, aplicativos legítimos podem ser bloqueados. Em tais situações, você pode configurar o Controle Ativo de Ameaças para não bloquear os mesmos aplicativos novamente criando regras de exclusão. Para saber mais, favor consultar “*Controle Ativo de Ameaças*” (p. 102).

15.1. Análise no acesso (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma gama de ameaças de malware ao analisar todos os arquivos acessados e mensagens de e-mail.

As predefinições da proteção em tempo real asseguram uma ótima proteção contra malware, com um impacto mínimo no desempenho do seu sistema. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos. Ou, no modo avançado, pode configurar as definições de análise em detalhe criando um nível de proteção personalizado.

15.1.1. Ligar ou desligar a proteção em tempo real

Para ativar ou desativar a proteção em tempo real contra o malware, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
4. Clique no botão para ativar ou desativar a análise no acesso.

5. Se você desejar desabilitar a proteção em tempo real, uma janela de alerta aparecerá. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a proteção em tempo real. Você pode desativar a proteção em tempo real por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema. A proteção em tempo real será ativada automaticamente quando o tempo selecionado expirar.

Atenção

Esta é uma incidência de segurança critica. Recomendamos que você desative a proteção em tempo-real o menos tempo possível. Quando a mesma está desativada você deixa de estar protegido contra as ameaças do malware.

15.1.2. Ajustar o nível de proteção em tempo real

O nível de proteção em tempo real determina as definições de análise da proteção em tempo real. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos.

Para ajustar o nível de proteção em tempo real, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
4. Arraste o cursor pela escala para definir o nível de proteção pretendido. Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

15.1.3. Configurar as definições da proteção em tempo-real

Os usuários avançados podem tirar proveito das configurações que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.

Para configurar as definições da proteção em tempo-real, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.

2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
4. Clique em **Personalizar**.
5. Configure as definições de análise como necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Você também pode encontrar informações úteis ao pesquisar na internet.
- **Opções de análise para arquivos acessados.** Pode configurar o Bitdefender para analisar todos os arquivos ou apenas os aplicativos (arquivos de programas) acessados. A análise de todos os arquivos acessados proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  Por padrão, ambas as pastas locais e compartilhamentos de rede estão sujeitos a análise no acesso. Para um melhor desempenho do sistema, você pode excluir os locais de rede da análise no acesso.

  As aplicações (ou arquivos de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de arquivos. Esta categoria inclui as seguintes extensões de arquivo:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analisar dentro dos arquivos compactados.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a proteção em tempo real. Os arquivos que contém arquivos infectados não são uma ameaça imediata à segurança do seu sistema. O malware só pode afetar o seu sistema se o arquivo infectado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada.

  Se decidir usar esta opção, você pode definir um tamanho limite aceitável para os arquivos analisados no acesso. Selecione a caixa correspondente e digite o tamanho máximo do arquivo (em MB).

- **Opções de verificação para e-mail e tráfego HTTP.** Para impedir que seja transferido malware para o seu computador, o Bitdefender analisa automaticamente os seguintes pontos de entrada de malware:
  - e-mails recebidos e enviados
  - Tráfego HTTP

  Analisar o tráfego na Internet poderá abrandar um pouco a navegação, mas vai bloquear o malware proveniente da Internet, incluindo transferências "drive-by".

  Embora não seja recomendado, você pode desativar a análise do antivírus de e-mail ou da internet para aumentar o desempenho do sistema. Se desactivar as respectivas opções de análise, as mensagens electrónicas e os arquivos recebidos e transferidos da Internet não serão analisados, permitindo que arquivos infectados sejam guardados no seu computador. Esta é uma ameaça grave pois a proteção em tempo real vai bloquear o malware quando os arquivos infectados forem acessados (abertos, movidos, copiados ou executados).

- **Verificar setor de boot.** Pode definir o Bitdefenderpara analisar os setores de saída do seu disco rígido. Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício. Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.

- **Analisar apenas arquivos novos e alterados.** Ao analisar apenas arquivos novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

- **Análise de keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicativos keylogger. Os keyloggers gravam o que você digita no seu teclado e enviam relatórios pela Internet para uma pessoa

maliciosa (hacker). O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e senhas, e usá-las em benefício pessoal.

- **Verificar na inicialização do sistema.** Selecionar a opção de verificação de inicialização antecipada na inicialização antes de que todos seus serviços essenciais sejam carregados. A missão desta ferramenta é melhorar a detecção de vírus na inicialização do sistema e o tempo de inicialização do sistema.

Ações efetuadas em malware detectado

Você poderá configurar as ações a serem realizadas pela proteção em tempo-real.

Para configurar as ações, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
4. Clique em **Personalizar**.
5. Selecione a aba **Ações** e defina as configurações de verificação como necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

As seguintes ações podem ser tomadas pela proteção em tempo-real do Bitdefender:

Tomar medidas adequadas

Bitdefender executará as ações recomendadas dependendo do tipo de arquivo detectado:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. O Bitdefender tentará remover automaticamente o código malware do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção.

  Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o

seu computador desaparece. Para mais informações, por favor consulte *"Gerenciar arquivos em quarentena"* (p. 100).

Importante
Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os arquivos suspeitos por não estar disponível uma rotina de desinfecção. Eles serão removidos para a quarentena para evitar uma potencial infecção.

  Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Arquivos que contêm arquivos infectados.**
  - Os arquivos que contêm apenas arquivos infectados são eliminados automaticamente.
  - Se um arquivo tiver arquivos infectados e limpos, o Bitdefender tentará eliminar os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.

Mover arquivos para a quarentena
Move os arquivos detectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informações, por favor consulte *"Gerenciar arquivos em quarentena"* (p. 100).

Negar acesso
Caso um arquivo infectado seja detectado, o acesso a ele será negado.

15.1.4. Restaurar configurações padrão

As predefinições da proteção em tempo real asseguram uma ótima proteção contra malware, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as configurações padrão de proteção em tempo real, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
4. Clique em **Padrão**.

15.2. Verificação solicitada

O objetivo principal do Bitdefender é manter seu computador livre de vírus. Isso é feito ao manter novos vírus fora de seu computador e verificar seus e-mails e novos arquivos copiados ao seu sistema.

Há o risco que um vírus já estar alojado em seu sistema, antes mesmo de você instalar o Bitdefender. É por isso que é uma ótima idéia verificar seu computador contra vírus residentes após instalar o Bitdefender. E é definitivamente uma boa idéia verificar seu computador frequentemente contra vírus.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objetos a serem analisados. Você pode analisar o computador sempre que desejar, executando as tarefas de análise padrão, ou as suas próprias tarefas de análise (tarefas definidas pelo usuário). Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.

15.2.1. Procurar malware em um arquivo ou pasta

Deve analisar os arquivos e as pastas sempre que suspeitar de uma infecção. Clique com o botão direito do sobre o arquivo ou pasta que pretende analisar, aponte para o **Bitdefender** e selecione **Analisar com o Bitdefender**. O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.

15.2.2. Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema. Normalmente, a realização de uma Análise Rápida

demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

Para executar uma Análise Rápida, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Análise Rápida**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

Ou mais rapidamente, clique no botão de ação **Análise Rápida** da interface do Bitdefender.

15.2.3. Executando uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o computador todos os tipos de malware que ameaçam a sua segurança, tais como vírus, spyware, adware, rookits e outros.

Nota

Como a **Análise do Sistema** realiza uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se executar esta tarefa quando não estiver usando o seu computador.

Antes de executar uma Análise do Sistema, recomendamos o seguinte:

- Certifique-se de que o Bitdefender apresente as assinaturas de malware atualizadas. Analisar o seu computador utilizando vacinas desatualizadas pode impedir que o Bitdefender detecte novos malwares criados desde a última atualização. Para mais informações, por favor consulte *“Mantendo o seu Bitdefender atualizado”* (p. 43).
- Encerre todos os programas abertos.

Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada. Para mais informações, por favor consulte *“Configurando uma análise personalizada”* (p. 89).

Para excutar uma Análise do Sistema, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise de Sistema**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

15.2.4. Configurando uma análise personalizada

Para configurar uma análise ao malware em detalhe e depois executá-la, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Gerenciar Verificações**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem escaneadas.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**. Uma nova janela aparece. Siga esses passos:
   a. Você pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido. Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

      Os usuários avançados podem tirar proveito das configurações que o Bitdefender oferece. Para configurar as opções de análise em detalhe, clique em **Personalizar**. Você encontrará informações sobre as mesmas no final desta seção.
   b. Também pode configurar as seguintes opções gerais:
      - **Executar a tarefa com prioridade Baixa .** Diminui a prioridade do processo de análise. Você permitirá que outros programas sejam executados mais rapidamente e aumentem o tempo de verificação.

- **Minimizar o Assistente de Análise para a área de notificação .** Minimiza a janela da análise para a área de notificação. Clique duplamente no ícone Bitdefender para abrir.
- Especifique a ação a aplicar se não forem encontradas ameaças.

c. Clique em **OK** para guardar as alterações e fechar a janela.

6. Se você deseja agendar a tarefa de verificação, use o botão **Agendar** na janela Básica. Escolha uma das opções correspondentes para definir uma agenda:
   - No início do sistema
   - Uma vez
   - Periodicamente
7. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise. Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.
8. Se quiser, você pode refazer rapidamente a verificação customizada anterior ao clicar na entrada correspondente na lista.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Você também pode encontrar informações úteis ao pesquisar na internet.
- **Verificar arquivos.** Pode configurar o Bitdefender para analisar todos os tipos de arquivos ou apenas os aplicativos (arquivos de programas). A análise de todos os arquivos proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

  As aplicações (ou arquivos de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de arquivos. Esta categoria inclui as seguintes extensões de arquivo: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar;

js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opções de análise para arquivos.** Os arquivos que contém arquivos infectados não são uma ameaça imediata à segurança do seu sistema. O malware só pode afetar o seu sistema se o arquivo infectado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada. No entanto, é recomendado que utilize esta opção para detectar e remover qualquer ameaça potencial, mesmo se não for imediata.

Nota
Analisar arquivos arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Verificar setor de boot.** Pode definir o Bitdefenderpara analisar os setores de saída do seu disco rígido. Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício. Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.
- **Analisar a Memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.
- **Analisar registro.** Selecione esta opção para analisar as chaves de registro. O Registo do Windows é uma base de dados que armazena as definições de configuração e as opções para os componentes do sistema operacional Windows, bem como para os aplicativos instalados.
- **Analisar cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu computador.
- **Analisar apenas arquivos novos e alterados.** Ao analisar apenas arquivos novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

- **Ignorar keyloggers comerciais.** Selecione esta opção se você tiver instalado e usar programas de controle e registro comerciais em seu computador. O programa de Controle e Registro comercial é um software legítimo de monitoramento do computador cuja função mais básica é registrar tudo o que é digitado no teclado.
- **Analisar em busca de rootkits.** Selecione esta opção para analisar rootkits e objetos ocultos usando tal software.

15.2.5. Assistente do analisador Antivírus

Ao iniciar uma análise a-pedido (por exemplo, clicar botão direito sobre a pasta, apontar para o Bitdefender e selecionar **Analisar com Bitdefender**), o assistente de análise antivírus Bitdefender irá aparecer. Siga o assistente para concluir o processo de análise.

Nota

Se o assistente de análise não aparecer, a análise pode estar configurada para executar silenciosamente no computador, enquanto você o utiliza. Você pode visualizar o ícone B Progresso da análise na área de notificação. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da mesma.

Passo 1 - Realizar Análise

Bitdefender iniciará a análise dos objetos selecionados. Você pode ver informação em tempo real sobre o status da análise e as estatísticas (incluindo o tempo decorrido, uma estimativa do tempo restante e o número de ameaças detectadas).

Espere que o Bitdefender termine a análise. O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Parando ou suspendendo a análise. Você pode interromper a análise no momento que quiser clicando em **Parar**. Você irá diretamente para o último passo do assistente. Para pausar temporariamente o processo de análise, clique em **Pausa**. Você deverá clicar em**Retomar** para retomar a análise.

Arquivos comprimidos protegidos por senha. Quando é detectado um arquivo protegido por senha, dependendo das definições da análise, poderá ter de indicar a senha. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. As seguintes opções estão disponíveis:

- **Senha.** Se você deseja que o Bitdefender analise o arquivo, selecione essa opção e digite a senha. Se você não sabe a senha, escolha uma das outras opções.
- **Não solicite uma senha e não analise este objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Pular todos os itens protegidos por senha.** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. O Bitdefender não será capaz de os analisar, porém um registro será mantido no relatório da análise.

Escolha a opção desejada e clique em **OK** para continuar a analisar.

Passo 2 - Escolher ações

Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.

Nota

Quando você executa uma análise rápida ou uma análise completa ao sistema, o Bitdefenderirá automaticamente executar as ações recomendadas nos arquivos detectados durante a análise. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

Os objetos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação sobre os objetos infectados.

Você pode escolher uma ação geral sendo executada para todos os problemas ou escolher ações separadas para cada grupo de problemas. Uma ou várias das seguintes opções podem aparecer no menu:

Tomar medidas adequadas

Bitdefender executará as ações recomendadas dependendo do tipo de arquivo detectado:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. O Bitdefender tentará remover automaticamente o código malware do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção.

Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informações, por favor consulte *"Gerenciar arquivos em quarentena"* (p. 100).

Importante

Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os arquivos suspeitos por não estar disponível uma rotina de desinfecção. Eles serão removidos para a quarentena para evitar uma potencial infecção.

  Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Arquivos que contêm arquivos infectados.**
  - Os arquivos que contêm apenas arquivos infectados são eliminados automaticamente.
  - Se um arquivo tiver arquivos infectados e limpos, o Bitdefender tentará eliminar os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.

Excluir

Remove os arquivos detectados do disco.

Se os arquivos infectados estiverem armazenados num arquivo junto com arquivos limpos, o Bitdefender tentará eliminar os arquivos infectados e reconstruir o arquivo com arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.

Não tome medida alguma

Nenhuma ação será tomada em arquivos detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses arquivos.

Clique em **Continuar** para aplicar as ações especificadas.

Passo 3 - Resumo

Quando o Bitdefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela. Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar Relatório** para ver o relatório da análise.

Clique em **Fechar** para fechar a janela.

Importante

Na maioria dos casos o Bitdefender desinfecta com sucesso o arquivo infectado ou isola a infecção. No entanto, há incidências que não puderam ser automaticamente resolvidas. Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente o malware, por favor consulte *"Remover malware do seu sistema"* (p. 191).

15.2.6. Ver os relatórios da análise

Sempre que uma análise for feita, um registro de análise é criado e o Bitdefender registra as incidências detectados na janela Antivírus. O relatório da análise contém informação detalhada sobre os processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

Pode abrir o relatório directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar um relatório de análise ou qualquer infecção detectada posteriormente, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** no menu suspenso correspondente.

Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo usuário e alterações de status para as análises automáticas.

3. Na lista de eventos, pode ver as análises que foram recentemente efetuadas. Clique no evento para visualizar detalhes sobre o mesmo.
4. Para abrir o registro de análise, clique em **Exibir registro** . Caso você deseje realizar a mesma verificação novamente, clique no botão **Verificar novamente**.

15.3. Análise automática de mídia removível

O Bitdefender detecta automaticamente quando você conectar um dispositivo de armazenamento removível em seu computador e analisa-o em segundo plano. Isto é recomendado, a fim de evitar vírus e outros malwares de infectarem seu computador.

Os dispositivos detectados se enquadram em uma destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pen drives e HDs externos.
- Diretórios de rede mapeados (remotos)

Você pode configurar a análise automática separadamente para cada categoria de dispositivos de armazenamento. A análise automática das drives de rede mapeadas está desativada por padrão.

15.3.1. Como funciona?

Quando detecta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existe malware em segundo plano (desde que a análise automática esteja ativada para aquele tipo de dispositivo). Um ícone de análise do Bitdefender B irá aparecer na barra do sistema Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da mesma.

Se o Piloto Automático estiver ativado, não será incomodado com a análise. A análise será apenas registrada e a informação sobre a mesma ficará disponível na janela Eventos.

Se o Piloto Automático estiver desativado:

1. Será notificado através de uma janela de pop-up que um novo dispositivo foi detectado e está a ser analisado.

2. Na maioria dos casos, o Bitdefender remove automaticamente o malware detectado ou isola os arquivos infectados na quarentena. Se houver ameaças não resolvidas depois da análise, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

Nota
Leve em conta que nenhuma ação pode ser efetuada nos arquivos que estiverem infectados ou suspeitos em CDs / DVDs. Do mesmo modo, nenhuma ação pode ser tomada nos arquivos infectados ou suspeitos que estejam nos drives da rede mapeada caso você não tenha os privilégios adequados.

3. Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para informar se você pode acessar com segurança aos arquivos nos dispositivos removíveis.

Esta informação pode ser útil para você:

- Tenha cuidado ao usar um CD/DVD infectado com malware, porque o malware não pode ser removido do disco (é apenas para leitura). Certifique-se que a proteção em tempo real está ativada para evitar que o malware se propague no seu sistema. Será melhor copiar os dados mais importantes do disco para o seu sistema e depois eliminá-los do disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover o malware de arquivos específicos devido a restrições legais ou técnicas. Exemplo disso são os arquivos guardados usando uma tecnologia patenteada (isto acontece porque o arquivo não pode ser recriado corretamente).

  Para saber como lidar com malware, por favor consulte "*Remover malware do seu sistema*" (p. 191).

15.3.2. Gerenciamento da análise de mídia removível

Para gerenciar a análise automática de mídia removível, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Exclusões**

Para uma melhor proteção, recomenda-se que ative a análise automática para todos os tipos de dispositivos de armazenamento removíveis.

As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Caso sejam detectados arquivos infectados, o Bitdefender tentará desinfectá-los (remover o código malware) ou movê-los para a quarentena. Se ambas as ações falharem, o assistente da Análise Antivírus permite especificar outras ações a serem adotadas com os arquivos infectados. As opções de análise são padrão e você não pode as alterar.

15.4. Configurar exceções da análise

O Bitdefender permite excluir arquivos, pastas ou extensões de arquivos específicos da análise. Esta característica visa evitar interferência ao seu trabalho e também pode ajudar a melhorar o desempenho do sistema. As exceções devem ser usadas por usuários com conhecimentos avançados de informática ou sob as recomendações de um representante da Bitdefender.

Pode configurar as exceções para aplicar apenas na análise no acesso ou a pedido, ou ambos. Os objetos excluídos da análise por demanda não serão analisados, independentemente deles serem acessados por você, ou por um aplicativo.

Nota

As exclusões NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise por demana: Você da um clique com o botão direito do mouse no arquivo ou diretório que pretende analisar e seleciona **Analisar com o Bitdefender**.

15.4.1. Excluir arquivos ou pastas da análise

Para excluir arquivos ou pastas específicas da análise, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione a aba **Exceções**.
5. Ative as exceções de análise para os arquivos que utilizem o respetivo botão.
6. Clique no link **Arquivos e pastas excluídos**. Na janela que surge, pode gerenciar os arquivos e pastas excluídos da análise.

7. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**. Alternativamente, pode digitar (ou copiar e colar) o caminho para o arquivo ou pasta no campo editar.
   c. Por padrão, o arquivo ou pasta selecionado é excluído tanto da análise no acesso quanto na análise a pedido. Para alterar o aplicativo da exclusão, selecione uma das outras opções.
   d. Clicando **Adicionar**.
8. Clique em **OK** para guardar as alterações e fechar a janela.

15.4.2. Excluir extensões de arquivos da análise

Quando exclui uma extensão de arquivo da análise, o Bitdefender deixará de analisar arquivos com essa extensão, independentemente da sua localização no seu computador. A exclusão também se aplica a arquivos em meios removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou drives da rede.

Importante
Tenha cuidado ao excluir as extensões da análise, porque tais exclusões podem tornar o seu computador vulnerável ao malware.

Para excluir extensões de arquivo da análise, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione a aba **Exceções**.
5. Ative as exceções de análise para os arquivos que utilizem o respetivo botão.
6. Clique no link **Extensões excluídas**. Na janela que surge, pode gerenciar o arquivo e extensões excluídos da análise.
7. Adicionar exceções seguindo estes passos:

a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.

b. Introduza as extensões que deseja excluir da análise, separando-as com ponto e vírgula (;). Eis um exemplo:

txt;avi;jpg

c. Por padrão, todos os arquivos com as extensões especificadas são excluídos da análise no acesso e a pedido. Para alterar o aplicativo da exclusão, selecione uma das outras opções.

d. Clicando **Adicionar**.

8. Clique em **OK** para guardar as alterações e fechar a janela.

15.4.3. Gerenciar exclusões de análise

Se as exclusões de análise configuradas já não forem necessárias, é recomendado que elimine ou desactive as exclusões da análise.

Para gerenciar as exceções da análise, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Exclusões** Use as opções na seção **Arquivos e pastas** para gerenciar as exceções de análise.
4. Para remover ou editar exceções da análise, clique em um dos links disponíveis. Proceder da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, dê um duplo clique na mesma (ou selecione-a e clique no botão **Editar**. Uma nova janela aparece quando você muda a extensão ou o caminho a ser excluído e o tipo de verificação que deseja que sejam excluídos, conforme necessário. Faça as alterações necessárias, depois clique em **Modificar**.
5. Para desativar exceções da análise, utilize o respectivo botão.

15.5. Gerenciar arquivos em quarentena

O Bitdefender isola os arquivos infectados com malware que não consegue desinfectar numa área segura denominada quarentena. Quando o vírus está

na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.

Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

Além disso, o Bitdefender analisa os arquivos em quarentena após cada atualização da vacina de malware. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

Para verificar e gerenciar arquivos da quarentena, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Quarentena**
4. Os arquivos da quarentena são gerenciados automaticamente pelo Bitdefender de acordo com as predefinições da quarentena. Embora não seja recomendado, pode ajustar as definições da quarentena de acordo com as suas preferências.

   Reanalisar quarentena após a atualização de definições de vírus
   Mantenha esta opção ativada para analisar automaticamente os arquivos da quarentena após cada atualização das definições de vírus. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

   Enviar arquivos suspeitos da quarentena para posterior análise.
   Mantenha esta opção ligada para enviar automaticamente os arquivos da quarentena para os Laboratórios da Bitdefender. As amostras de arquivos serão analisadas pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

   Apagar conteúdo com mais de {30} dias
   Por definição, arquivos de quarentena mais antigos que 90 dias são automaticamente apagados. Se quiser alterar este intervalo, digite um novo valor no campo correspondente. Para desabilitar a exclusão automática dos antigos arquivos em quarentena, digite 0.

5. Para eliminar um arquivo da quarentena, selecione-o e clique no botão **Eliminar**. Se pretende restaurar um arquivo da quarentena para a respectiva localização original, selecione-o e clique em **Restaurar**.

15.6. Controle Ativo de Ameaças

O Controle Ativo de Ameaças da Bitdefender é uma tecnologia de detecção proativa inovadora que usa métodos heurísticos avançados para detectar ameaças potenciais em tempo real.

O Controle Ativo de Ameaças monitora continuamente os aplicativos em execução no computador, procurando ações semelhantes a malwares. Cada uma destas ações é classificada e é calculada uma pontuação geral para cada processo. Quando a classificação geral para um processo atinge um dado limite, o processo é considerado perigoso e é bloqueado automaticamente.

Se o Piloto Automático estiver desativado, você será notificado através de uma janela pop-up sobre o aplicativo bloqueado. Caso contrário, o aplicativo será bloqueado sem qualquer notificação. Você pode verificar quais aplicativos foram detectados pelo Controle Ativo de Ameaças na janela Eventos.

15.6.1. Verificar aplicativos detectados

Para checar os aplicativos detectados pelo Controle Ativo de Ameaças, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** no menu suspenso correspondente.
3. Clique no evento para visualizar detalhes sobre o mesmo.
4. Se você confiar no aplicativo, pode configurar o Controle Ativo de Ameaças para não bloqueá-lo mais clicando em **Permitir e monitorar**. O Controle Ativo de Ameaças continuará a monitorar aplicativos excluídos. Caso um aplicativo excluído seja detectado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

15.6.2. Ligando ou desligando o Controle Ativo de Ameaças

Para ligar ou desligar o Controle Ativo de Ameaças, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione a aba **Shield**.
5. Clique no botão para ligar ou desligar o Controle Ativo de Ameaças.

15.6.3. Ajustando a proteção do Controle Ativo de Ameaças

Se você perceber que o Controle Ativo de Ameaças detecta aplicativos legítimos com frequência, você deve definir um nível de proteção mais permissivo.

Para ajustar a proteção do Controle Ativo de Ameaças, arraste o marcador ao longo da escala para definir o nível de proteção desejado.

Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

Nota
Ao definir um nível de proteção mais alto, o Controle Ativo de Ameaças irá solicitar alguns sinais de comportamentos semelhantes a malwares para relatar um processo. Isto provocará um aumento do número de aplicativos que são comunicados e, ao mesmo tempo, um aumento da probabilidade de falsos positivos (aplicativos limpos detectados como maliciosos).

15.6.4. Gerenciar processos excluídos

Você pode configurar regras de exclusão para aplicativos confiáveis de forma que o Controle Ativo de Ameaças não os bloqueie se apresentarem comportamentos semelhantes a malwares. O Controle Ativo de Ameaças continuará a monitorar aplicativos excluídos. Caso um aplicativo excluído seja detectado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

Para gerenciar exclusões de processos do Controle Ativo de Ameaças, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Exclusões**
4. Clique no link **Processos excluídos**. Na janela que aparece, você pode gerenciar as exclusões de processos do Controle Ativo de Ameaças.

   Nota
   As exclusões de processo também se aplicam a Detecção de Invasão.

5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione o aplicativo que quer excluir e depois clique em **OK**.
   c. Mantenha a opção **Permitir** selecionada para prevenir que o Controle Ativo de Ameaças bloqueie o aplicativo.
   d. Clicando **Adicionar**.
6. Para remover ou editar exceções, proceda da seguinte forma:
   - Para apagar um item da lista, escolha-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, dê um duplo clique na mesma (ou selecione-a e clique no botão **Modificar**. Faça as alterações necessárias, depois clique em **Modificar**.
7. Salvar as alterações e fechar a janela.

16. ANTISPAM

Spam é o termo utilizado para descrever mensagens electrónicas não solicitadas. Spam é um problema crescente, tanto para usuários quanto para empresas. Não é bonito, você não gostaria que seus filhos vissem, pode fazer você perder o emprego (por desperdiçar muito tempo ou por receber e-mails impróprios no e-mail do escritório) e você não pode impedir as pessoas de enviá-lo. A melhor coisa a fazer é, obviamente, parar de recebê-los. Infelizmente, spams chegam em inúmeras formas e tamanhos, e em grandes quantidades.

O Bitdefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam padrão para limpar o spam antes de o mesmo chegar à caixa de correio A receber do usuário. Para mais informações, por favor consulte *"Compreender o Antispam"* (p. 106).

A proteção Antispam do Bitdefender está disponível apenas para clientes de correio eletrônico configurado para receber mensagens de e-mail via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.

Nota

O Bitdefender não proporciona protecção antispam para contas de correio eletrônico a que acede através de sítios de Internet (webmail).

As mensagens não solicitadas detectadas pelo Bitdefender são marcadas com o prefixo [SPAM] no campo do assunto. O Bitdefender move automaticamente mensagens de spam para um diretório específico, como abaixo:

- No Microsoft Outlook, as mensagens de spam são movidas para um diretório **Spam**, localizado no diretório **Itens Excluídos**. O diretório **Spam** é criado durante a instalação do Bitdefender.
- No Outlook Express e Windows Mail, as mensagens de spam são movidas diretamente para a pasta **Itens Excluídos**.
- No Mozilla Thunderbird, as mensagens de spam são movidas para uma pasta **Spam**, localizada na pasta **Lixeira**. O diretório **Spam** é criado durante a instalação do Bitdefender.

Se você utiliza outros clientes de e-mail, você deve criar uma regra para mover as mensagens de e-mail marcadas como [SPAM] pelo Bitdefenderpara uma pastade quarentena customizada.

16.1. Compreender o Antispam

16.1.1. Filtros Anti-spam

O Motor Antispam do Bitdefender inclui proteção em nuvem e outros filtros diferenciados que asseguram que sua Caixa de Entrada fique livre de SPAM, como a Lista de Amigos, Spammers list e Filtro de Caracteres.

Lista de Amigos / Lista de Spammers

A maioria das pessoas se comunica regularmente com um grupo de pessoas ou mesmo recebe mensagens de empresas e organizações do mesmo domínio. Usando as **listas de amigos ou spammers**, você pode facilmente classificar de quais pessoas você quer receber e-mails (amigos) não importa o que a mensagem contenha, ou de quais pessoas você nem quer ouvir falar (spammers).

Nota

Nós recomendamos que você adicione os nomes e e-mails de seus amigos à **Lista de Amigos**. O Bitdefendernão bloqueia mensagens das pessoas nesta lista; portanto, adicionar amigos assegura que e-mails legítimos vão chegar ao destino.

Filtro de Caracteres

Muitas mensagens de spam estão escritas em caracteres cirílicos e/ou asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-as como SPAM.

16.1.2. Operação Antispam

O mecanismo do Bitdefender Antispam utiliza todos os filtros antispam combinados para determinar se uma determinada mensagem de e-mail deverá entrar em sua **Caixa de Entrada** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o e-mail é movido diretamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista de Spammers irá apoderar-se do seu correio eletrônico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Em seguida, o Filtro de caracteres checa se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Caso esteja o e-mail será marcado como SPAM e movido para a pasta **Spam**.

Nota

Se o e-mail é marcado como SEXUALLY EXPLICIT na linha do assunto, o Bitdefender vai considerá-lo SPAM.

16.1.3. Clientes de e-mail e protocolos suportados

A proteção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP. No entanto a barra de ferramentas do Antispam Bitdefender apenas se integra em:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (em sistemas de 32 bits)
- Mozilla Thunderbird 3.0.4

16.2. Ligar ou desligar a proteção antispam

A proteção Antispam está ativada por padrão.

Para desativar o módulo de antispam, faça o seguinte:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antispam**, depois clique no botão para ativar ou desativar o **Antispam**.

16.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

Na parte superior do seu programa de e-mail você pode ver a barra de ferramentas Antispam. A Barra de Ferramentas Antispam ajuda a gerenciar a proteção antispam diretamente do seu cliente de e-mail. Você pode facilmente corrigir o Bitdefender se ele marcou uma mensagem legítima como spam.

Importante

O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para *"Clientes de e-mail e protocolos suportados"* (p. 107).

Cada botão será explicado abaixo:

Configurações - abre uma janela onde pode configurar as definições da barra de ferramentas e dos filtros antispam.

É Spam - indica que o e-mail selecionado é spam. O e-mail será removido imediatamente para a pasta **Spam**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

Não Spam - indica que o e-mail selecionado não é spam e o Bitdefender não deveria tê-lo identificado como tal. O e-mail será movido da pasta **Spam** para o diretório **Caixa de entrada** . Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

Importante

O botão **Não é Spam** fica ativo quando você escolhe uma mensagem marcada como Spam pelo Bitdefender (normalmente essas mensagens estão localizadas na pasta **Spam**).

Adicionar Spammer - adicina o remetente do e-mail selecionado para a lista de Spammers. Você poderá ter que clicar **OK** para acusar recebimento. As mensagens de e-mail recebidas destes endereços na lista de Spammers, são automaticamente marcados como [spam].

Adicionar Amigo - adiciona o remetende do e-mail selecionado à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.

Spammers- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informações, por favor consulte *"Configurar a lista de Spammers"* (p. 111).

Amigos - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo. Para mais informações, por favor consulte *"Configurar a Lista de Amigos"* (p. 110).

16.3.1. Indicar os erros de detecção

Se você está usando um cliente de e-mail suportado, você pode facilmente corrigir o filtro antispam (indicando qual mensagem de e-mail não deve ser marcada como [spam]). Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique o botão **Adicionar Amigos** na barra de ferramentas do antispam do Bitdefender para adicionar o remetente à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). A mensagem de e-mail será removida para a pasta de Entrada.

16.3.2. Indicar mensagens de spam não detectadas

Se você está usando um cliente de e-mail suportado, você pode facilmente indicar quais mensagens de e-mail foram detectadas como spam. Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a Pasta de Entrada.
3. Selecione as mensagens spam não detectadas.
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). Elas são marcadas imediatamente como [spam] e movidas para a pasta lixo.

16.3.3. Configurar definições da barra de ferramentas

Para definir as configurações da barra de ferramentas antispam para o seu cliente de e-mail, clique no botão **\Configurações** na barra de ferramentas e depois no separador **Configurações da Barra de Ferramentas**.

Você tem as seguintes opções:

- **Mova a mensagem para os Itens Eliminados** (apenas para o Microsoft Outlook Express / Windows Mail)

Nota
No Microsoft Outlook / Mozilla Thunderbird, as mensagens de spam são automaticamente movidas para uma pasta de Spam, localizada nos Itens Eliminados / pasta Lixeira.

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marque as mensagens indesejadas como ler automaticamente, de forma que não sejam um incômodo quando chegarem.
- Você pode optar por visualizar ou não janelas de confirmação quando clica nos botões **Adicionar Spammer** e **Adicionar Amigo** na barra de ferramentas antispam.

  As janelas de confirmação podem evitar a adição acidental de destinatários de e-mail à lista de Amigos / Spammers.

16.4. Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de quem você sempre deseja receber mensagens, não importa o conteúdo. Mensagens de seus amigos não são marcadas como Spam, mesmo se o conteúdo se assemelhe a Spam.

Nota
Qualquer mensagem vinda de um endereço contido na **Lista de amigos**, será automaticamente entregue em sua Caixa de entrada sem mais processamentos.

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clique no botão **Amigos** na barra de ferramentas antispam do Bitdefender.
- Em alternativa, proceda da seguinte forma:

  1. Clique no ícone no canto inferior direito da interface do Bitdefender.
  2. Selecione a aba **Proteção**.
  3. No módulo **Antispam**, selecione **Gerenciar Amigos**.

Para adicionar um endereço de e-mail, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar.** Syntax: nome@domínio.com.

Para adicionar os endereços eletrônicos de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e depois clique em **Adicionar**. Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;
- *com - todos os e-mails contendo o sufixo de domínio com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do endereço eletrônico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique no link **Remover** correspondente. Para apagar todas as entradas da lista, clique no botão **Limpar Lista**.

Você pode salvar a lista de Amigos em um arquivo que poderá ser usado em outro computador ou após a reinstalação do produto. Para salvar a lista de Amigos, clique no botão **Salvar** e salve o arquivo no local desejado. O arquivo terá a extensão .bwl .

Para carregar a lista de amigos salva anteriormente, clique no botão **Carregar** e abra o arquivo .bwl correspondente. Para redefinir o conteúdo da lista existente ao carregar uma lista salva anteriormente, selecione **Sobrescrever lista atual**.

Clique em **OK** para guardar as alterações e fechar a janela.

16.5. Configurar a lista de Spammers

Lista de Spammers é uma lista de todos os endereços de quem você não quer receber mensagens, não importa qual o conteúdo. Qualquer mensagem vinda de um e-mail na **Lista de Spammers** será marcado como Spam, sem pais processamentos.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clique no botão **Spammers** na barra de ferramentas antispam do Bitdefender integrado no seu cliente de correio eletrônico.
- Em alternativa, proceda da seguinte forma:
  1. Clique no ícone no canto inferior direito da interface do Bitdefender.
  2. Selecione a aba **Proteção**.
  3. No módulo **Antispam**, selecione **Gerenciar Spammers**.

Para adicionar um endereço de e-mail, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar.** Syntax: nome@domínio.com.

Para adicionar os endereços eletrônicos de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e depois clique em **Adicionar**. Syntax:

- @domínio.com, *domínio.com e domínio.com - todos os e-mails vindos de domínio.com serão marcados como Spam;
- *domínio* - todos os e-mails vindos de domínio (não importa quais os sufixos do domínio) serão marcados como Spam;
- *com - todos os e-mails contendo o sufixo de domínio com serão marcados como Spam.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

Atenção

Não adicione domínios de serviços de e-mail legítimos (tais como Yahoo!, Gmail, Hotmail, ou outros) à lista de spammers. Caso contrário, os e-mails recebidos de qualquer usuário registrado de tais serviços serão detectados como spams. Se, por exemplo, você adicionar o yahoo.com à lista de Spammers, todos os e-mails vindos deste yahoo.com endereço serão marcados como [spam].

Para eliminar um item da lista, clique no link **Remover** correspondente. Para apagar todas as entradas da lista, clique no botão **Limpar Lista**.

Você pode salvar a lista de Spammers em um arquivo que poderá ser usado em outro computador ou após a reinstalação do produto. Para salvar a lista de Spammers, clique no botão **Salvar** e salve o arquivo no local desejado. O arquivo terá a extensão .bwl .

Para carregar uma lista de Spammers salva anteriormente clique no botão **Carregar** e abra o arquivo .bwl correspondente. Para redefinir o conteúdo da lista existente ao carregar uma lista salva anteriormente, selecione **Sobrescrever lista atual**.

Clique em **OK** para guardar as alterações e fechar a janela.

16.6. Configurando filtros antispam locais

Como descrito em *"Compreender o Antispam"* (p. 106), o Bitdefender utiliza um conjunto de diferentes filtros antspam para identificar o spam. Os filtros antispam são pré-configurados para uma protecção eficaz.

Importante

Dependendo se recebe ou não mensagens electrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desactive ou active a definição que bloqueia automaticamente estas mensagens. A respectiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar os filtros locais antispam, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antispam**, depois clique nos botões para ativar ou desativar os filtros antispam locais.

Se estiver usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, poderá configurar os filtros locais antispam diretamente a partir do seu cliente de email. Clique no botão **Configurações** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente) e depois no separador **Filtros Antispam**.

16.7. Configurando os Ajustes em Nuvem

Na detecção na nuvem faz uso dos Serviços na Nuvem do Bitdefender para lhe proporcionar uma proteção antispam eficaz e sempre atualizada.

As funções de proteção em nuvem enquanto mantiver o Antispam Bitdefender ativado.

As amostras de e-mails legítimos ou spam podem ser enviados para a Nuvem Bitdefender quando você indica erros de detecção ou e-mails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra de e-mail para Nuvem Bitdefender através da seleção das opções desejadas, ao seguir estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antispam**, depois selecione as opções desejadas na aba **Configurações**.

Se estiver usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, pode configurar a detecção na nuvem diretamente a partir do seu cliente de email. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente) e depois no separador **Definições de Nuvem**.

17. PROTEÇÃO DA INTERNET

A Proteção da Internet do Bitdefender garante uma experiência de navegação segura, alertando-o sobre possíveis páginas de phishing.

O Bitdefender fornece proteção da Internet em tempo real para:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Para definir a configuração da Proteção da Internet, siga esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Proteção da Internet**.

Clique nos botões para ligar ou desligar:

- O consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um ícone ao lado de cada resultado:

  Você não deve visitar esta página da rede.

  Esta página pode ter conteúdo perigoso. Tenha cautela caso decida visitá-la.

  Esta página é segura.

  O Consultor de Pesquisa qualifica os resultados da pesquisa dos seguintes motores de busca:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  O Consultor de Pesquisa classifica os links publicados nos seguintes serviços de redes sociais:
  - Facebook
  - Twitter
- Analisar tráfego web SSL.

Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. É, por isso, recomendado que ative a análise SSL.

- Proteção contra fraudes.
- Proteção contra phishing.

Você pode criar uma lista de páginas que não serão analisadas pelos mecanismos antimalware, antiphishing e antifraude do Bitdefender. A lista deve conter apenas os websites em que você confia plenamente. Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Para configurar e gerenciar páginas usando a proteção da Internet fornecida pelo Bitdefender, clique no link **Lista Segura**. Uma nova janela aparece.

Para adicionar um site à lista segura, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site desta lista, selecione-o na lista e clique no link **Remover** correspondente.

Clique **Salvar** para salvar as alterações e fechar a janela.

17.1. Alertas de Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site e a ameaça detectada.

Você precisa decidir o que fará a seguir. As seguintes opções estão disponíveis:

- Navegue para fora da página web clicando em **Leve-me de volta à segurança**.
- Desativar o bloqueio de páginas que contenham phishing ao clicar em **Desativar filtro Antiphishing**.
- Desative o bloqueio de páginas que contenham malware ao clicar em **Desativar filtro Antimalware**.
- Adicione a página à lista segura Antiphishing, clicando em **Adicionar à Lista Branca**. Esta página já não será analisada pelos motores Antiphishing do Bitdefender.
- Prosseguir para a página web, apesar do aviso, clicando em **eu compreendo os riscos, avançar assim mesmo** .

18. PROTEÇÃO DE DADOS

18.1. Apagar arquivos permanentemente

Ao apagar um arquivo, o mesmo já não fica acessível por meios normais. No entanto o arquivo continua armazenado no disco rígido até que seja sobrescrito com a cópia de novos arquivos.

O Destruidor de Arquivos do Bitdefender o ajuda a apagar dados permanentemente removendo-os fisicamente de seu disco rígido.

Pode rapidamente destruir arquivos ou pastas do seu computador usando o menu contextual Windows, seguindo estes passos:

1. Clique botão direito sobre o arquivo ou pasta que deseja apagar permanentemente.
2. Selecione **Bitdefender** > **Destruidor de Arquivos** no menu contextual que aparece.
3. Uma janela de confirmação aparecerá. Clique em **Sim** para iniciar o assistente do Destruidor de Arquivos.
4. Aguarde que o Bitdefender termine a destruição dos arquivos.
5. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

Alternativamente você pode destruir os arquivos a partir da interface do Bitdefender.

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. No módulo **Proteção de Dados**, selecione **Destruidor de Arquivos**.
4. Siga o assistente do Destruidor de Arquivos:
   a. **Adicionar Pasta(s)**

      Adicione os arquivos ou as pastas que pretende remover permanentemente.

   b. Clique em **Próximo** e confirme que você deseja continuar com o processo.

      Aguarde que o Bitdefender termine a destruição dos arquivos.

c. **Resultados**

   Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

19. VULNERABILIDADE

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operacional e as aplicações que usa regularmente. Também deve considerar desativar as definições do Windows que tornam o sistema mais vulnerável ao malware. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, senhas fortes (senhasque não são fáceis de adivinhar) devem de ser criadas para cada conta de usuário do Windows.

O Bitdefender verifica automaticamente o seu sistema por vulnerabilidades e alerta você sobre elas. As vulnerabilidades do sistema incluem o seguinte:

- aplicativos desatualizados em seu computador.
- Falta de atualizações do Windows.
- Senhas fracas para contas de usuário do Windows.

O Bitdefender proporciona duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Você pode analisar o seu sistema em busca de vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Se usar a monitorização da vulnerabilidade automática, pode verificar e resolver vulnerabilidades detectadas na janela Eventos.

Você deve verificar e corrigir vulnerabilidades do sistema a cada uma ou duas semanas.

19.1. Procurar vulnerabilidades no seu sistema

Para corrigir as vulnerabilidades do sistema usando a opção Análise de Vulnerabilidade, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Vulnerabilidade**, selecione **Análise de Vulnerabilidade**.
4. Espere o Bitdefender analisar as vulnerabilidades do seu sistema. Para interromper o processo de análise, clique no botão **Pular** na parte inferior da janela.

Ou mais rapidamente, clique no botão de ação **Análise de Vulnerabilidade** da interface do Bitdefender.

- **Atualizações Críticas do Windows**

  Clique em **Ver detalhes** para ver uma lista de atualizações críticas do Windows que não estão instaladas em seu computador.

  Para iniciar a instalação das atualizações selecionadas, clique em **Instalar atualizações**. Note que a instalação das atualizações poderá demorar um pouco e algumas delas podem exigir a reinicialização do sistema para concluir a instalação. Se necessário, reinicie o sistema quando lhe convier.

- **Atualizações do aplicativo**

  Caso um aplicativo não esteja atualizado, clique no link **Fazer download da nova versão** para fazer download da última versão.

  Clique em **Ver detalhes** para ver informações sobre o aplicativo que precisa ser atualizado.

- **Senhas fracas de contas do Windows**

  Pode ver a lista dos usuários de contas Windows configurados no seu computador e o nível de proteção que as suas senhas garantem.

  Clique em **Alterar senha ao fazer login** para definir uma nova senha para seu sistema.

  Clique em **Ver detalhes** para modificar as senhas fracas. Você pode escolher entre pedir ao usuário para alterar a senha no próximo acesso ou alterar a senha imediatamente. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

No canto superior direito da janela, você pode filtrar os resultados de acordo com suas preferências.

19.2. Usando o monitoramento automático de vulnerabilidade

O Bitdefender analisa regularmente as vulnerabilidades do seu sistema, em segundo plano, e mantém registros das incidências detectadas na janela Eventos.

Para verificar e resolver os problemas detectados, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Vulnerabilidade** na lista Selecione Eventos.
3. Pode ver a informação detalhada sobre as vulnerabilidades detectadas do sistema. Dependendo da incidência, para consertar uma vulnerabilidade específica, proceda da seguinte forma:
   - Caso haja alguma atualização do Windows disponível, clique em **Atualizar agora**.
   - Se as atualizações automáticas do Windows estiverem desabilitadas, clique em **Habilitar**.
   - Se um aplicativo estiver desatualizado, clique em **Atualizar agora** para obter a conexão com a página da Internet do fornecedor, onde poderá instalar a versão mais recente desse aplicativo.
   - Se uma conta de usuário do Windows tiver uma senha vulnerável, clique em **Alterar senha** para obrigar o usuário a mudar a senha no próximo logon ou você mesmo alterar a senha. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Caso a função do Windows Autorun esteja ativada, clique em **Reparar** para desativá-la.

Para configurar as definições de monitoração de vulnerabilidade, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Vulnerabilidade**.
4. Clique no botão para ativar ou desativar a análise de Vulnerabilidade.

Importante

Para ser notificado automaticamente sobre vulnerabilidades do sistema ou de aplicativos, mantenha a opção **Análise de Vulnerabilidade** ativada.

5. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

Atualizações Críticas do Windows
: Verifique se o seu sistema operacional Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

Atualizações do aplicativo
: Verifique se os aplicativos instalados em seu sistema estão atualizados. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

Senhas inadequadas
: Verifique se as senhas das contas Windows configuradas no sistema são fáceis de descobrir ou não. A configuração de senhas difíceis de descobrir (senhas altamente seguras) torna muito difícil a invasão do seu sistema pelos hackers. Uma senha segura inclui letras maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Execução automática de conteúdos multimídia
: Verifique o status do recurso Windows Autorun. Esta característica permite que os aplicativos se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

  Alguns tipos de malware usam Autorun para se propagar automaticamente na mídia removível do PC. Por isso, recomenda-se desativar este recurso do Windows.

Nota

Se desativar a monitoração de uma vulnerabilidade específica, as incidências relacionadas deixarão de ser registradas na janela de Eventos.

20. FIREWALL

O Firewall protege o seu computador contra tentativas de conexão de saída e entrada não autorizadas, seja em redes locais ou Internet. É bastante semelhante a um guarda à sua porta - mantém o controle de tentativas de conexão e decide o que permitir e o que bloquear.

A firewall do Bitdefender usa um conjunto de regras para filtrar dados transmitidos para ou a partir do seu sistema. As regras estão organizadas em 2 categorias:

Regras Gerais
: Regras que determinam os protocolos através dos quais a comunicação é permitida.

  É usado um conjunto de regras padrão que proporciona uma ótima proteção. Você pode editar as regras permitindo ou impedindo as conexões através de determinados protocolos.

Regras de Aplicativos
: As regras que determinam como cada aplicativo pode acessar os recursos da rede e à Internet.

  Em condições normais, o Bitdefender cria automaticamente uma regra sempre que um aplicativo tenta acessar a Internet. Também pode adicionar ou editar manualmente regras dos aplicativos.

O Bitdefender atribui automaticamente um tipo de rede a cada conexão de rede que detecta. Dependendo do tipo de rede, a proteção firewall é definida ao nível apropriado para cada ligação.

Para saber mais sobre as configurações da firewall para cada tipo de rede e como editar as configurações de rede, por favor consulte *"Gerenciando Configurações de Conexão"* (p. 128).

20.1. Ligar ou desligar a proteção firewall

Para ativar ou desativar a proteção firewall, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall**, depois clique no botão Firewall.

Atenção

Devido ao fato de expor o seu computador a conexões não autoriadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.

20.2. Gerenciando regras do Firewall

20.2.1. Regras gerais

Sempre que determinados dados são transmitidos pela Internet, são usados certos protocolos.

As regras gerais permitem-lhe configurar os protocolos através dos quais o tráfego é permitido. Por padrão, as regras gerais não são exibidas ao abrir o Firewall. Para editar regras, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela do **Firewall**, selecione a aba **Regras**.
5. Marque a caixa **Exibir regras gerais** no canto inferior esquerdo da janela.

As regras padrão são exibidas. Para editar a prioridade de uma regra, clique na seta correspondente na coluna **Permissão** e selecione **Permitir** ou **Negar**.

DNS sobre UDP / TCP

Permitir ou negar DNS sobre o UDP e o TCP.

Este tipo de conexão é permitido por padrão.

Enviando e-mails

Permite ou nega envio de email por SMTP.

Este tipo de conexão é permitido por padrão.

Navegação na Rede HTTP

Permitir ou impedir navegação na web HTTP.

Este tipo de conexão é permitido por padrão.

Entrada de ICMP / ICMPv6

Permitir ou impedir mensagens ICMP / ICMPv6.

As mensagens ICMP são frequentemente usadas pelos hackers para atacarem as redes de computadores. Este tipo de conexão é permitido por padrão.

Entrada de Conexões Remotas ao Desktop

Permitir ou impedir o acesso de outros computadores em Conexões Remotas de Desktop.

Este tipo de conexão é permitido por padrão.

Tráfego do Windows Explorer em HTTP / FTP

Permitir ou impedir tráfego HTTP ou FTP do Windows Explorer.

Este tipo de conexão é permitido por padrão.

20.2.2. Regras da aplicação

Para visualizar e gerenciar o acesso dos aplicativos de controle das regras de firewall aos recursos de rede e à Internet, siga esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela do **Firewall**, selecione a aba **Regras**.

Pode ver na tabela os programas (processos) para os quais as regras de firewall foram criadas. Para verificar as regras criadas para um aplicativo específico, clique nele duas vezes.

Para cada regra é apresentada a seguinte informação:

- **Nome** - o nome do processo ao que as regras se aplicam.
- **Tipo de Rede** - os tipos de adaptador de rede e processo aos que as regras se aplicam. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por padrão, as regras se aplicam a qualquer rede. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de um aplicativo através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Protocolo** - o protocolo IP aos quais as regras se aplicam. Por padrão, as regras se aplicam a qualquer protocolo.

- **Permissão** - se o acesso do aplicativo à rede ou à Internet é permitido ou negado sob circunstâncias específicas.

Para gerenciar as regras, use os botões acima da tabela:

- **Adicionar regra** - abre uma janela onde você pode criar uma regra nova.
- **Remover regra** - apaga a regra selecionada.
- **Redefinir regras** - abre uma janela onde você pode optar por remover as regras atuais e restaurar as padrão.

Adicionar / editar regras de aplicativo

Para adicionar ou editar uma regra de aplicativo, clique no botão **Adicionar regra** acima da tabela ou clique em uma regra atual. Uma nova janela aparece. Proceder da seguinte forma:

Na aba **Configurações** você pode aplicas as seguintes mudanças:

- **Caminho do Programa.** Clique em **Explorar** para selecionar o aplicativos a qual a regra se aplica.
- **Tipo de rede.** Selecione o tipo de rede ao qual a regra se aplica. Pode alterar o tipo abrindo o menu pendente **Tipo de Rede** e selecionando um dos tipos disponíveis na lista.

Tipo de rede	Descrição
Confiável	Desativa o firewall para o respectivo dispositivo.
Casa/Escritório	Permite o tráfego entre o seu computador e os computadores na rede local.
Público	Todo o tráfego é filtrado.
Não Confiável	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
Permitir	O aplicativo especificado será permitido o acesso à rede / Internet nas circunstâncias determinadas.

Permissão	Descrição
Negar	O aplicativo especificado será negado o acesso à rede / Internet nas circunstâncias determinadas.

Na aba **Avançado** você pode customizar as seguintes mudanças:

- **Endereço Local Customizado.** Especifique o endereço IP local e a porta aos quais a regra se aplica.
- **Endereço Remoto Customizado.** Especifique o endereço IP remoto e a porta à qual a regra se aplica.
- **Direção.** Selecione do menu a direção do tráfego ao qual a regra se aplica.

Direção	Descrição
Saída	As regras valem apenas para tráfego de saída.
Entrada	As regras valem apenas entrada.
Ambos	As regras valem para as duas direções.

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Qualquer uma**.
  - Se você quiser que a regra se aplique a TCP, selecione **TCP**.
  - Se você quiser que a regra se aplique a UDP, selecione **UDP**.
  - Se quiser que a regra se aplique em um protocolo específico, digite o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.

Nota

Os números dos protocolos IP são atribuidos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em http://www.iana.org/assignments/protocol-numbers.

20.3. Gerenciando Configurações de Conexão

Para cada conexão de rede você pode configurar zonas especiais confiáveis ou não confiáveis.

Uma zona confiável é um dispositivo em que você confia plenamente, por exemplo um computador ou uma impressora. Todo o tráfego entre o seu computador e um dispositivo confiável é permitido. Para partilhar recursos com determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.

Uma zona não confiável é um dispositivo que você não quer de forma alguma que se comunique com o seu computador.

Para visualizar e gerenciar zonas na sua rede de adaptadores, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela do **Firewall**, selecione a aba **Adaptadores**.

Os adaptadores de rede com conexões ativas e as áreas atuais, se houver, são exibidos nesta aba.

Para cada zona a seguinte informação é exibida:

- **Tipo de Rede** - o tipo de rede a que o seu computador está ligado.
- **Modo Invisível** - para não ser detectado por outros computadores.

  Para configurar o Modo Stealth, selecione a opção desejada do menu suspenso.

Opção Stealth	Descrição
Ligado	O Modo Stealth está ligado. O seu computador é invisível a partir da rede local e da Internet.
Desligado	O Modo Stealth está desligado. Qualquer pessoa da rede local ou da Internet pode fazer ping e detectar o seu computador.

- **Genérico** - se as regras genéricas são aplicadas a esta ligação.

Se o endereço IP de um adaptador é alterado, o Bitdefender modifica o tipo de rede de acordo com a alteração. Caso deseje manter o mesmo tipo, selecione **Sim** do menu suspenso correspondente.

Adicionar / editar exceções

Para adicionar ou editar exceções, clique no botão **Exceções de rede** acima da tabela. Uma nova janela exibindo os Adaptadores disponíveis conectados à rede aparecerá. Proceder da seguinte forma:

1. Selecione o endereço IP do computador que deseja adicionar, ou digite um endereço ou intervalo de endereço na caixa de texto fornecida.
2. Selecione a permissão:
   - **Permitir** - para autorizar o tráfego entre o seu computador e o computador seleccionado.
   - **Negar** - para bloquear o tráfego entre o seu computador e o computador seleccionado.
3. Clique no botão **+** para adicionar a exceção, fechar a janela.

   Se quiser remover um IP, clique no botão correspondente e feche a janela.

20.4. Configurando definições avançadas

Para configurar as definições avançadas de firewall, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela do **Firewall**, selecione a aba **Configurações**.

A ferramenta a seguir pode ser habilitada ou desabilitada.

- **Bloquear scans de portas na rede** - detecta e bloqueia tentativas de encontrar quais portas estão abertas.

  Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador. Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.

20.5. Configurar intensidade de alertas

Bitdefender Internet Security 2016 foi desenvolvido para ser o mínimo intrusivo possível. Em condições normais, não é necessario tomar decisões sobre permitir ou impedir conexões ou ações tentadas pelos aplicativos em execução no seu sistema.

Se quiser ter o controle completo sobre a decisão tomada, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela **Configurações Gerais** selecione a aba **Configurações Gerais**.
3. Ligar **Modo Paranóico** clicando no botão correspondente.

> **Nota**
> Quando o Modo Paranoico estiver ligado, os recursos Autopilot e Perfis serão desligados automaticamente.
> O **Modo Paranoico** poderá ser usado simultaneamente com o **Modo de Bateria**.

Enquanto o Modo Paranoico estiver ligado, você receberá notificações para tomar ações cada vez que acontecer o seguinte:

- Um aplicativo tenta conexão à Internet.
- Um aplicativo tenta realizar uma ação considerada suspeita pela Detecção de Invasão ou pelo Controle Ativo de Ameaças.

O alerta contém informações detalhadas sobre o aplicativo e o comportamento detectado. Selecione **Permitir** ou **Impedir** a ação usando o botão respectivo.

21. DETECÇÃO DE INVASÃO

A Detecção de Invasão do Bitdefender monitora as atividades da rede e do sistema em caso de atividades maliciosas ou violações de política. Pode detectar e bloquear as tentativas de alterar arquivos críticos do sistema, arquivos do Bitdefender ou entradas de registro, a instalação de drivers de malware ou ataques efetuados por injeção de código (injeção da DLL).

Para configurar a Detecção de Invasão, siga esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Detecção de Invasão**.
4. Para ativar a Detecção de Invasão, clique no botão correspondente.
5. Arraste o cursor pela escala para definir o nível de agressividade pretendido. Utilize a descrição do lado direito da escala para escolher o nível que melhor se adequa às suas necessidades de segurança.

Você pode verificar quais aplicativos foram detectados pela Detecção de Invasão na janela Eventos.

Se existirem aplicativos confiáveis que você não quer que a Detecção de Invasão analise, você pode adicionar regras de exclusão para eles. Para excluir um aplicativo da análise, siga os passos descritos na seção *“Gerenciar processos excluídos”* (p. 103).

Nota

A operação de Detecção de Invasão é relacionada a do Controle Ativo de Ameaças. As regras de exclusão de processo aplicam-se a ambos os sistemas.

22. PROTEÇÃO CONTRA RANSOMWARE

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis travando-os e logo exigindo dinheiro para permitir que o usuário retome controle de seu sistema. Esse software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o usuário, induzindo-o a realizar o pagamento solicitado.

A infecção pode se espalhar por meio de e-mails de spam, downloads de anexos ou ao se visitarem sites infectados e instalar aplicativos maliciosos sem informar ao usuário sobre o que está ocorrendo com seu sistema.

Ransomwares podem ter um dos seguintes comportamentos, prevenindo que o usuário acesse seu sistema:

- Encriptar dados privados e pessoais sem a possibilidade de desencriptação até que um resgate seja pago pela vítima.
- Travar a tela do computador e exibir uma mensagem pedindo dinheiro. Neste caso, nenhum arquivo é encriptado, mas o usuário é forçado a realizar o pagamento.
- Bloquear a execução de aplicativos.

Utilizando a última tecnologia, a Proteção contra Ransomwares do Bitdefender assegura a integridade do sistema ao proteger áreas essenciais do sistema contra danos, sem prejudicar o desempenho do sistema. Contudo, você pode desejar proteger seus arquivos pessoais, como documentos, fotos, filmes ou os arquivos que você armazena na nuvem.

22.1. Ativar ou desativar a Proteção contra Ransomwares

Para desativar o módulo de Proteção contra Ransomwares siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique em **Proteção Ransomware**.
4. Clique no botão para ativar ou desativar a **Proteção Ransomware**.

Sempre que um aplicativo tentar acessar um arquivo protegido, um pop-up do Bitdefender será exibido. Você poderá permitir ou negar o acesso.

22.2. Proteja seus arquivos pessoais contra ataques de ransomwares

Caso você deseje armazenar arquivos pessoais em um abrigo, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Proteção Ransomware** e então clique no botão **Pastas protegidas**.
4. Clique em **Adicionar** e procure a pasta que deseja proteger.
5. Clique em **OK** para adicionar a pasta selecionada ao ambiente de proteção.

As configurações de fábrica já protegem as pastas Documentos, Imagens, Documentos públicos e Imagens públicas contra ataques de malware. Dados pessoais armazenados em serviços online de armazenamento de arquivos, como Box, Dropbox, Google Drive e OneDrive também são adicionados ao ambiente de proteção, desde que seus aplicativos estejam instalados no sistema.

Nota
Pastas personalizadas somente podem ser protegidas para os usuários atuais. Arquivos de sistema e de aplicativos não podem ser adicionadas às exceções.

22.3. Configurando os aplicativos confiáveis

A proteção contra ransomware pode ser desativada para alguns aplicativos, mas apenas aqueles em que você confia devem ser adicionados à lista.

Para adicionar aplicativos confiáveis às exceções, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Proteção Ransomware**, selecione **Aplicativos confiáveis**.
4. Clique em **Adicionar** e procure os aplicativos que deseja proteger.
5. Clique em **OK** para adicionar o aplicativo selecionado ao ambiente de proteção.

22.4. Configurando os aplicativos bloqueados

Dentre os aplicativos que você instalou em seu computador, alguns podem desejar acessar seus arquivos pessoais.

Para restringir esses aplicativos, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Proteção Ransomware**, selecione **Aplicativos bloqueados**.
4. Clique em **Adicionar** e procure os aplicativos que deseja restringir.
5. Clique em **OK** para adicionar o aplicativo selecionado à lista de restrições.

22.5. Proteção na inicialização

Sabe-se que muitos aplicativos de malware são configurados para serem executados na inicialização do sistema, o que pode danificar seriamente uma máquina. A Proteção na inicialização do Bitdefender verifica todas as áreas essenciais do sistema antes que todos os arquivos sejam carregados, sem impacto no desempenho do sistema. Simultaneamente, é fornecida proteção contra certos ataques que dependem da execução de códigos em stack ou heap, injeções de código ou ganchos em certas bibliotecas dinâmicas.

Para desativar a Proteção na inicialização, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique em **Proteção Ransomware**.
4. Clique no botão para ativar ou desativar a **Proteção na inicialização**.

23. SEGURANÇA SAFEPAY PARA TRANSAÇÕES ONLINE

O computador está rapidamente se tornando a principal ferramenta para compras e operações bancárias online. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba o envio de dados pessoais, dados de contas bancárias e cartão de crédito, senhas e outros tipos de informação privada pela Internet; em outras palavras, exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em obter. Os hackers são incansáveis nos seus esforços para roubar estas informações, portanto todo cuidado é pouco em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente projetado para manter a sua atividade bancária, suas compras on-line e qualquer outra transação online privada e segura.

Para a melhor proteção à privacidade, o Gerenciador de Senhas do Bitdefender foi integrado ao Bitdefender Safepay™ para proteger suas credenciais sempre que você desejar acessar locais privados online. Para mais informações, por favor consulte *"Proteção do Gerenciador de Senhas para suas credenciais"* (p. 140).

O Bitdefender Safepay™ oferece os seguintes recursos:

- O mesmo bloqueia o acesso à sua área de trabalho e qualquer tentativa de capturar imagens de sua tela.
- Ele protege suas senhas enquanto você navega.
- O mesmo apresenta um teclado virtual que, quando usado, torna impossível para os hackers lerem as teclas que usar.
- É completamente independente dos outros navegadores.
- Vem com uma proteção de hotspot embutida para ser usada quando o seu computador se conecta a redes Wi-fi não-seguras.
- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.
- Não está limitado ao banking e às compras online. Qualquer página web pode ser aberta no Bitdefender Safepay™.

23.1. Usando o Bitdefender Safepay™

Por padrão, o Bitdefender detecta quando você entra em uma página de banco ou de compras em qualquer navegador de seu computador e pergunta se você gostaria de usar o Bitdefender Safepay™.

Para acessar a interface principal do Bitdefender Safepay™, utilize um dos métodos a seguir:

- Na interface do Bitdefender:
  1. Clique no botão de ação **Safepay** da interface do Bitdefender.
- Do Windows:
  - No **Windows 7**:
    1. Clique **Iniciar** e acesse **Todos os Programas**.
    2. Clique em **Bitdefender**.
    3. Clique em **Bitdefender Safepay™**.
  - No **Windows 8 e Windows 8.1**:

    Encontre o Bitdefender Safepay™ na tela inicial do Windows (por exemplo, você pode digitar "Bitdefender Safepay™" diretamente na tela Inicial) e então clique no ícone.
  - No **Windows 10**:

    Digite "Bitdefender Safepay™" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente.

Nota

CAso o plug-in do Adobe Flash Player não esteja instalado ou esteja desatualizado, será apresentada um mensagem do Bitdefender. Clique no botão correspondente para continuar.

Após o processo de instalação, você terá que reabrir o navegador Bitdefender Safepay™ manualmente para continuar o seu trabalho.

Se você estiver acostumado com navegadores de Internet, não terá nenhum problema para usar o Bitdefender Safepay™ - ele parece e se comporta como um navegador comum:

- digite as URLs que deseja acessar na barra de endereços.

- adicione abas para visitar múltiplas páginas na janela do Bitdefender Safepay™ clicando em .
- navegue para a frente e para trás e atualize as páginas usando respetivamente.
- acesse configurações do Bitdefender Safepay™ clicando em e escolhendo **Configurações**.
- proteja suas senhas com o Gerenciador de senhas clicando em .
- gerencie seus bookmarks clicando em ao lado da barra de endereço.
- abra o teclado virtual clicando em .
- aumente ou diminua o tamanho do navegador pressionando as teclas **Ctrl** e **+/-** simultaneamente no teclado numérico.
- veja informações sobre seu Bitdefender clicando em e escolhendo **Sobre**.
- imprima as informações importantes clicando .

23.2. Configurando definições

Clique em e escolha **Configurações** para configurar o Bitdefender Safepay™:

Configurações Gerais

Escolha o que deve de ser feito ao acessar a um site online de compras ou de bancos no seu navegador habitual:

- Abrir sites automaticamente no Safepay.
- Recomendar-me a usar o Safepay.
- Não me recomendar o uso do Safepay.

Lista de domínios

Escolha como o Bitdefender Safepay™ irá se comportar quando você visitar páginas com domínios específicos no seu navegador adicionando-os à lista de domínios e selecionando o comportamento para cada um:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender avise sobre a ação a ser tomada.
- Nunca utilizar o Bitdefender Safepay™ ao visitar uma página do domínio em um navegador comum.

Bloqueando pop-ups

Você pode optar por bloquear pop-ups clicando no botão correspondente.

Você também pode criar uma lista de páginas que possam exibir pop-ups. A lista deve conter apenas os websites em que você confia plenamente.

Para adicionar uma página à lista, insira seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover um site desta lista, selecione-o na lista e clique no link **Remover** correspondente.

Permitir proteção de hotspot.

Você pode permitir uma proteção extra quando estiver conectado a redes Wi-fi inseguras habilitando esta ferramenta.

Acesse *"Proteção Hotspot em redes não-seguras."* (p. 139) para mais informações.

23.3. Gerenciando bookmarks

Caso você tenha desabilitado a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente não detectar algumas páginas, você pode adicionar favoritos ao Bitdefender Safepay™ para que você possa abrir as suas páginas favoritas com facilidade no futuro.

Siga estes passos para adicionar um URL aos favoritos do Bitdefender Safepay™

1. Clique no ícone ao lado da barra de endereços para abrir a página de Favoritos.

Nota
A página de Favoritos abre por padrão quando você executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.
3. Inserir o URL e o título do bookmark e clique em **Criar**. Marque a opção **Abrir automaticamente no Safepay** se você quiser que a página favorita abra com o Bitdefender Safepay™ todas as vezes que você acessá-la. A URL é também adicionada à lista de Domínios na página de definições.

23.4. Proteção Hotspot em redes não-seguras.

Ao usar o Bitdefender Safepay™ em redes de Wi-fi inseguras (por exemplo, um hotspot público), uma proteção extra é oferecida pelo recurso Proteção de Hotspot. Este serviço criptografa as comunicações de Internet em conexões não-seguras, ajudando assim a manter a sua privacidade sem importar a que rede esteja ligado.

A proteção de hotspot funciona apenas se o seu computador estiver conectado a uma rede insegura.

A conexão segura será inicializada e uma mensagem irá aparecer na janela do Bitdefender Safepay™ quando a conexão for feita. O símbolo aparece à frente da URL na barra de endereços para o ajudar a identificar facilmente as conexões seguras.

Para melhorar sua experiência de navegação, você pode habilitar os plug-ins do **Adobe Flash** e do **Java** clicando em **Mostrar configurações avançadas**.

Pode ser necessário confirmar a ação.

24. PROTEÇÃO DO GERENCIADOR DE SENHAS PARA SUAS CREDENCIAIS

Utilizamos os nossos computadores para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em aplicativos de mensagens instantâneas.

Mas como todos sabemos, nem sempre é fácil memorizar a senha!

E se não formos cuidadosos ao navegar online, as nossas informações privadas, tais como endereço de e-mail, ID de mensagens instantâneas ou os dados do cartão de crédito podem ficar comprometidas.

Guardar as suas senhas ou os seus dados pessoais numa folha ou no computador pode ser perigoso, pois estes podem ser acessados e utilizados por pessoas que desejam roubar e utilizar essas informações. E memorizar todas as senhas definidas para as suas contas online ou para os seus websites favoritos não é uma tarefa fácil.

Portanto, há alguma forma de garantir que encontramos as nossas senhas quando necessitamos das mesmas? E podemos ter a certeza de que as nossas senhas secretas estão sempre seguras?

O Gerenciador de Senhas o ajuda a lembrar de suas senhas, protege sua privacidade e fornece uma navegação segura.

Utilizando uma única senha mestre para acessar suas credenciais, o Gerenciador de Senhas facilita sua vida protegendo suas senhas em uma Carteira.

Para oferecer a melhor proteção às suas atividades online, o Gerenciador de Senhas é integrado ao Bitdefender Safepay™ e fornece uma solução unificada para os vários meios em que seus dados podem ser comprometidos.

O Gerenciador de Senhas protege as seguintes informações privadas:

- Informações pessoais, tais como endereço de e-mail e número de telefone
- Credenciais de login para websites
- Informações de contas bancárias ou o número do cartão de crédito
- Dados de acesso às contas de e-mail
- Senhas para os aplicativos

- Senhas para redes Wi-Fi

24.1. Configuração do Gerenciador de Senhas

Após a conclusão da instalação e ao abrir seu navegador, você será notificado através de uma janela pop-up que poderá utilizar a Carteira para uma experiência de navegação mais simples.

A Carteira do Bitdefender é onde você pode armazenar seus dados pessoais.

Clique em **Explorar** para iniciar o assistente de configuração da Carteira. Siga o assistente para concluir o processo de configuração.

Duas tarefas podem ser realizadas durante este passo:

- Crie uma nova base de dados de Carteira para proteger suas senhas.

  Durante o processo de configuração, será solicitada a proteção da sua Carteira com uma senha principal. A nova senha deve ser forte e conter pelo menos 7 caracteres

  Para criar uma senha segura, utilize no mínimo um número ou símbolo e uma maiúscula. Após definir a senha, caso alguém tente acessar à Carteira, será necessário primeiro digitar a senha.

  Após definir a senha mestre, você tem a opção de sincronizar as informações na Carteira com a nuvem, para que você possa utilizá-las em todos os seus dispositivos.

  Ao final do processo de configuração, as seguintes definições da Carteira estão ativadas por predefinição:

  - **Salvar credenciais automaticamente na Carteira**.
  - **Solicitar minha senha mestre quando eu fizer login no meu computador**.
  - **Bloquear a Carteira automaticamente quando deixar meu PC sozinho.**.
- Importe uma base de dados existente, caso já tenha utilizado a Carteira no seu sistema anteriormente.

Exportar a base de dados da Carteira

Para exportar a base de dados da Carteira, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.

3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Carteiras.**
4. Selecione o banco de dados da Carteira desejado na seção **Minhas Carteiras** e então clique no botão **Exportar**.
5. Siga os passos para exportar a base de dados da Carteira para uma localidade no seu sistema.

Nota
A Carteira precisa estar aberta para que o botão **Exportar** esteja disponível.

Crie uma nova base de dados da Carteira

Para criar uma nova base de dados de Carteira, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Carteiras.**
4. Clique no ícone + na janela que aparecerá.
5. Na área **Começar do zero**, clique em **Criar nova**.
6. Digite as informações necessárias nos campos correspondentes.
   - Título da Carteira - digite um nome personalizado para seu banco de dados da Carteira.
   - Senha Mestre - digite uma senha para sua Carteira.
   - Redigitar Senha - redigite a senha que você definiu.
   - Dica - digite uma dica para lembrar de sua senha.
7. Clique em **Continuar**.
8. Nesta etapa, você pode escolher armazenar suas informações na nuvem. Se você selecionar Sim, suas informações bancárias permanecerão armazenadas localmente em seu dispositivo. Escolha a opção desejada e então clique em **Continuar**.
9. Selecione o navegador da Internet de onde você deseja importar credenciais.
10. Clique em **Finalizar**.

Sincronize suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Carteiras**.
4. Selecione o banco de dados da Carteira desejado na seção **Minhas Carteiras** e então clique no botão **Configurações**.
5. Escolha a opção desejada na janela que aparecer, e então clique em **Salvar**.

Nota
A Carteira precisa estar aberta para que o botão **Configurações** esteja disponível.

Gerenciar as suas credenciais da Carteira

Para gerenciar suas senhas, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Carteiras**.
4. Selecione o banco de dados da Carteira desejado na seção **Minhas Carteiras** e então clique no botão **Abrir**.

Uma nova janela aparece. Selecione a categoria desejada na parte superior da janela:

- Identidade
- Websites
- Online banking
- E-mails
- Aplicativos
- Redes Wi-Fi

Adicionar/ editar as credenciais

- Para adicionar uma nova senha, escolha a categoria desejada acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão Salvar.
- Para editar uma entrada da lista, selecione-a e clique no botão **Editar**.
- Para sair, clique em **Cancelar**.
- Para remover uma entrada, selecione-a, clique no botão **Editar** e escolha **Apagar**.

24.2. Ativando e desativando a proteção do Gerenciador de Senhas

Para ativar ou desativar a proteção do Gerenciador de Senhas, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas**.
4. Clique na chave **Status do módulo** para ativar ou desativar o Gerenciador de Senhas.

24.3. Alterando as configurações do Gerenciador de Senhas

Para configurar a senha principal detalhadamente, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Configurações de segurança**.

As seguintes opções estão disponíveis:

- **Solicitar a minha senha mestre sempre que eu acessar o meu PC** - você será solicitado a inserir a senha mestre ao acessar o computador.

- **Solicitar senha principal ao abrir navegadores e aplicativos** - será solicitada a senha principal ao acessar um navegador ou aplicativo.
- **Bloquear automaticamente a Carteira quando deixa o meu PC sem supervisão** - será solicitada a senha principal quando regressar ao seu computador após 15 minutos.

> **Importante**
> Não se esqueça da sua senha mestre e guarde-a num local seguro. Caso esqueça a senha, será necessário reinstalar o programa ou contatar o suporte do Bitdefender.

Melhore a sua experiência

Para selecionar os navegadores ou os aplicativos em que você deseja integrar o Gerenciador de Senhas, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Plugins**.

   Marque um aplicativo para utilizar o Gerenciador de Senhas e melhorar sua experiência:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Skype
   - Yahoo! Messenger

Configurando o Preenchimento Automático

O recursos Preenchimento Automático simplifica a conexão aos seus websites favoritos ou login nas suas contas online. Na primeira fez que você inserir suas informações de login e informações pessoais em um navegador de Internet, eles estarão automaticamente protegidos na Carteira.

Para configurar as definições do **Preenchimento Automático**, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. Clique no módulo **Gerenciador de Senhas** e então selecione a aba **Configurações de preenchimento automático**.
4. Configure as seguintes opções:
   - **Preenchimento Automático de Credenciais de Login**:
     - **Preencher automaticamente e sempre as credenciais de início de sessão** - as credenciais são inseridas automaticamente no browser.
     - **Deixe-me decidir quando quero preencher o meu login automaticamente** - você pode escolher quando preencher as credenciais automaticamente no seu navegador.
   - **Configure como o Gerenciador de Senhas protege suas credenciais**:
     - **Salvar as credenciais automaticamente na Carteira** - as credenciais de login e outras informações pessoais como os detalhes do seu cartão de crédito e detalhes pessoais são salvos e atualizados automaticamente na sua Carteira.
     - **Perguntar-me sempre** - você será sempre perguntado se pretende adicionar as suas credenciais à Carteira.
     - **Não salvar, atualizarei as informações manualmente** - as credenciais só podem ser atualizadas na Carteira manualmente.
   - **Formulários de preenchimento automático**:
     - **Mostre minhas opções de preenchimento quando eu visitar uma página com as formulários** - um pop-up com as opções de preenchimento aparecerá sempre que o Bitdefender detectar que você deseja realizar um pagamento on-line ou fazer um login.

Controle as informações do Gerenciador de Senhas de seu navegador

Você pode controlar facilmente as informações do Gerenciador de Senhas diretamente de seu navegador, para ter fácil acesso a todos os dados importantes. O plugin da Carteira do Bitdefender é suportado pelos seguintes navegadores: Google Chrome, Internet Explorer e Mozilla Firefox, e também é integrado ao Safepay.

Para acessar a extensão da Carteira do Bitdefender, abra seu navegador, permita a instalação do plugin e clique no ícone na barra de ferramentas.

A extensão da Carteira do Bitdefender contém as seguintes opções:

- Abrir Carteira - abre a Carteira.
- Fechar Carteira - fecha a Carteira.
- Páginas web - abre um submenu com todos os logins de sites armazenados na Carteira. Clique em **Adicionar página** para adicionar novas páginas à lista.
- Preencher formulário - abre o submenu contendo a informação adicionada para uma categoria específica. Aqui você pode adicionar novos dados à sua Carteira.
- Gerador de Senhas - permite que você gere senhas aleatórias que você pode utilizar para contas novas e existentes. Clique em **Mostrar configurações avançadas** para personalizar a complexidade da senha.
- Configurações - abre a janela de configurações do Gerenciador de Senhas.
- Relatar problema - relate quaisquer problemas que encontrar com o Gerenciador de Senhas do Bitdefender.

25. CONSULTOR PARENTAL

A função de Consultor Parental permite que você controle o acesso à Internet e a aplicativos específicos para cada dispositivo que tenha a função instalada. Uma vez que você tenha configurado o Consultor Parental, você poderá descobrir facilmente o que seu filho está fazendo nos dispositivos que usa e onde ele esteve nas últimas 24 horas. Ademais, para ajudá-lo a saber melhor o que seu filho está fazendo, o aplicativo apresenta estatísticas sobre suas atividades e interesses.

Tudo o que precisa é um computador com acesso à Internet e um navegador de Internet.

Você pode configurar o Consultor Parental para bloquear:

- Páginas web inapropriadas.
- aplicações tais como: jogos, programas de partilha de arquivos e outros.
- bloquear contatos específicos que são proibidos de entrar em contato telefônico com seu filho.

Verifique as atividades de seus filhos e altere as configurações do Consultor Parental utilizando a Bitdefender Central desde qualquer computador ou dispositivo móvel conectado à Internet.

25.1. Acessando o Consultor Parental - Meus Filhos

Quando você acessar a seção do Consultor Parental, a janela **Meus filhos** estará disponível. Aqui você pode visualizar e editar todos os perfis que criou para seus filhos. Os perfis aparecem como cartões de perfil, permitindo que você os controle com rapidez e verifique seu estado atual com apenas uma olhada.

Assim que você criar um perfil, poderá personalizar configurações mais detalhadas para monitorar e controlar o acesso à Internet e a aplicativos específicos para seus filhos.

Você pode acessar as configurações de Consultor Parental em sua conta Bitdefender Central de qualquer computador ou dispositivo móvel conectado à Internet.

Acesse sua conta online:

- Em qualquer dispositivo com acesso à Internet:

1. Acesse sua conta Bitdefender Central.

   Assegure-se de acessar a conta com suas creden

2. Selecione o painel **Consultor Parental**.
3. Na janela **Meus filhos** que aparecerá, você pode controlar e configurar os perfis do Consultor Parental para cada dispositivo.

- A partir de sua interface Bitdefender:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Privacidade**.
3. No módulo **Consultor Parental**, selecione **Configurar**.

   Você será redirecionado à página da Bitdefender Central. Assegure-se de acessar a conta com suas creden

4. Selecione o painel **Consultor Parental**.
5. Na janela **Meus filhos** que aparecerá, você pode controlar e configurar os perfis do Consultor Parental para cada dispositivo.

Nota

Certifique-se que tem a sessão iniciada com a conta de administrador. Somente usuários com privilégios administrativos no sistema (administradores) podem acessar e configurar o Consultor Parental.

25.2. Adicionando o perfil do seu filho

Para começar a monitorar as atividades de seus filhos, você precisa configurar um perfil e instalar o Agente Consultor Parental do Bitdefender em dispositivos que ele utiliza.

Para adicionar o perfil do seu filho ao Consultor Parental:

1. Acesse o painel Consultor Parental de sua conta Bitdefender Central.
2. Clique em **ADICIONAR PERFIL** na lateral direita da janela **Meus dispositivos**.
3. Preencha os campos com informações específicas, como: nome, e-mail, sexo e data de nascimento, e então clique em **CONTINUAR**.

Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as especificações consideradas apropriadas para sua faixa etária.

4. Caso o dispositivo de seu filho já possua o Bitdefender Internet Security 2016 instalado, selecione esse dispositivo da lista disponível e clique em **CONTINUAR**.

   Caso o dispositivo de seu filho não tenha nenhum Bitdefender com a função de Consultor Parental incluído, clique em **Adicionar novo dispositivo**. Selecione o sistema operacional desse dispositivo e clique em **CONTINUAR**.

   Digite o endereço de e-mail para onde devemos enviar o link de download de instalação do aplicativo Consultor Parental do Bitdefender.

   Em dispositivos com Windows, o Bitdefender Internet Security 2016 que você incluiu em sua assinatura deverá ser baixado e instalado. Em dispositivos Android, o Agente Consultor Parental do Bitdefender deverá ser baixado e instalado.

25.2.1. Vinculando o Consultor Parental à Bitdefender Central

Para monitorar a atividade online de seus filhos no Android, você deve vincular seu dispositivo à sua Bitdefender Central, acessando a conta no aplicativo.

Para associar o aparelho a sua conta Bitdefender Central, siga estes passos:

1. Abra o aplicativo de Consultor Parental.
2. Marque a caixa **Eu declaro ser o proprietário legal deste dispositivo** e pressione **Próximo**.
3. Acesse sua conta Bitdefender Central existente.

   Caso não tenha uma conta, escolha criar uma nova conta utilizando o botão correspondente.

Nota

Você também poderá digitar um nome para seu aparelho. Caso você associe mais de um dispositivo à sua conta, isso irá ajudar a identificar os aparelhos mais facilmente.

4. Pressione **Link**.
5. Selecione o perfil da criança que você deseja monitorar da lista e pressione **Continuar**.

   Você também pode pressionar **Adicionar nova criança** para criar um novo perfil e preencher os campos necessários.
6. Ative os privilégios de administrador para o aplicativo, pressionando **Ativar**.

   Isso prevenirá que seu filho desinstale o Agente Consultor Parental.

25.2.2. Monitorando a atividade da criança

O Bitdefender ajuda a manter o registro do que seus filhos estão fazendo online.

Desse modo, você sempre poderá descobrir exatamente que páginas eles visitaram, que aplicativos utilizaram ou que atividades foram bloqueadas pelo Consultor Parental.

Dependendo das configurações que você definir, os relatórios podem conter informações detalhadas sobre cada evento, como:

- O status do evento.
- A severidade da notificação.
- O nome do dispositivo.
- A data e a hora em que ocorreu o evento.

Para monitorar o tráfego de Internet, os aplicativos acessados ou a atividade de Facebook do seu filho, faça o seguinte:

1. Acesse o painel Consultor Parental de sua conta Bitdefender Central.
2. Selecione o cartão de dispositivo desejado.

   Na janela Linha do tempo você poderá visualizar a informação que lhe interessa.

25.2.3. Configurando os Ajustes Gerais

O Consultor Parental já vem configurado de fábrica para registrar as atividades dos seus filhos.

Para receber notificações por e-mail, faça o seguinte:

1. Acesse o painel Consultor Parental de sua conta Bitdefender Central.
2. Clique no ícone no campo superior direito.
3. Habilite a opção correspondente para receber relatórios de atividade.
4. Introduza o endereço eletrônico para onde serão enviadas das notificações por correio eletrônico.
5. Ajuste a frequência selecionando: semanal ou mensal.
6. Receber notificações via e-mail para os seguintes:
   - Sites bloqueados
   - App bloqueadas
   - Contactos MI bloqueados
   - SMS de um contato bloqueado
   - Chamada recebida de um número bloqueado
   - Remoção do aplicativo de Consultor Parental para Facebook
7. Clique em **Guardar**.

25.2.4. Editando um perfil

Para editar um perfil existente:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone no cartão de perfil desejado, e então selecione **Editar**.
4. Após personalizar as configurações desejadas, selecione **Salvar**.

25.2.5. Removendo um perfil

Para remover um perfil existente:

1. Acesse sua conta Bitdefender Central.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone no cartão de perfil desejado, e então selecione **Remover**.

25.3. Configurando perfis do Consultor Parental

Para iniciar o monitoramento de seus filhos, um perfil deverá ser designado ao dispositivo que tem o Agente Consultor Parental do Bitdefender instalado.

Após criar um perfil para seu filho, você poderá personalizar configurações mais detalhadas para monitorar e controlar o acesso à Internet e a aplicativos específicos.

Para iniciar a configuração de um perfil, selecione o cartão de perfil desejado na janela **Meus filhos**.

Clique em uma aba para configurar a função correspondente do Consultor Parental para o dispositivo:

- Linha do tempo - exibe as atividades, interesses, locais e interações com amigos, a partir do dia corrente.
- Atividades - permite que você bloqueie o acesso a certos aplicativos, como jogos, programas de mensagens instantâneas, filmes, etc.
- Interesses - permite que você filtre a navegação e estabeleça limites de tempo para o acesso à Internet.
- Amigos - aqui você pode especificar que contatos da lista de seu filho têm permissão para contatá-lo por telefone.
- Lugares - aqui você pode definir que lugares são seguros ou não para seu filho.
- Social - permite que você bloqueie o acesso a redes sociais.

25.3.1. PAINEL

A janela Linha do tempo fornece informações detalhadas sobre as atividades de seus filhos nas últimas 24 horas, dentro e fora de casa.

A janela Linha do tempo inclui informações sobre:

- **Locais** - aqui você pode visualizar os locais onde seu filho esteve durante o dia. Clique no link **Definir horário de hibernar** para definir um horário em que o monitoramento de atividades seja alterado automaticamente para o modo standby.
- **Interesses** - aqui você pode visualizar informações sobre que categorias de páginas da Internet seu filho visitou. Clique no link **Revisar conteúdo inapropriado** para acessar os conteúdos inapropriados que ele assistiu.

- **Interações sociais** - aqui você pode visualizar um diagrama de barras com um resumo das atividades ao longo do dia.
- **Atividades** - aqui você pode visualizar os contatos que ligaram para o seu filho, as informações que ele compartilhou no Facebook e os novos amigos que ele acrescentou à sua rede.
- **Aplicativos** - aqui você pode visualizar os aplicativos que seu filho utilizou.

Nota
Para informações detalhadas, clique na opção desejada localizada no canto direito de cada seção.

25.3.2. Atividades

A janela Atividades o ajuda a impedir a execução de aplicativos. Jogos, mídia e programas de mensagens instantâneas, assim como outras categorias de programa podem ser bloqueadas deste modo.

O módulo pode ser ativado ou desativado utilizando o botão correspondente.

Para configurar o Controle de Aplicativo para uma conta de usuário específica, siga estes passos:

1. Uma lista com cartões será exibida. Os cartões representam os aplicativos que seu filho utiliza.
2. Selecione o cartão com o aplicativo que você deseja que seu filho pare de utilizar.

   O símbolo de marcação que aparecerá indica que seu filho não poderá utilizar o aplicativo.

25.3.3. Interesses

A janela de Interesses o ajuda a bloquear sites com conteúdo inapropriado. Sites que hospedam vídeos, jogos, mídia e programas de mensagens instantâneas, assim como outras categorias de conteúdo negativo, podem ser bloqueadas desse modo.

O módulo pode ser ativado ou desativado utilizando o botão correspondente.

Dependendo da idade que você definiu para seu filho, a lista de Interesses já vem com uma variedade de categorias ativas. Para permitir ou negar acesso a uma categoria específica, clique nela.

Dependendo da idade que você definiu para seu filho, a lista de Interesses já vem com uma variedade de categorias ativas.

Permitir ou bloquear um website

Para permitir ou negar acesso a uma categoria específica, clique nela.

1. Clique no botão **GERENCIAR**.
2. Digite o endereço da página que deseja permitir ou bloquear no campo correspondente.
3. Selecione **Permitir** ou **Negar**.
4. Clique em **Ok** para salvar as alterações.

25.3.4. Amigos

A janela Amigos permite que você especifique quais amigos da lista de contatos de seu filho têm permissão para contatá-lo por telefone.

Para restringir um número específico de um amigo, primeiro você precisa adicionar o número de seu filho ao seu perfil:

1. Selecione a aba **Consultor Parental** em sua conta Bitdefender Central.
2. Clique no ícone ⋮ no cartão de perfil desejado, e então selecione **Editar**.
3. Digite o número de telefone de seu filho no campo correspondente, e então clique em **SALVAR**.
4. Selecione o perfil da criança para qual deseja estabelecer restrições.
5. Selecione a aba **Amigos**.

   Uma lista com cartões será exibida. Os cartões representam os contatos do telefone de seu filho.
6. Selecione o cartão com o número de telefone que você deseja bloquear.

   O símbolo de marcação que aparecerá indica que seu filho não receberá ligações do número de telefone selecionado.

Para bloquear números desconhecidos, ative a opção **nenhuma interação de identificação de chamadas**.

25.3.5. Lugares

Visualizar a localização atual do dispositivo no Google Maps. A localização é atualizada a cada 5 segundos, para que você possa rastreá-lo se estivesse em movimento.

A precisão da localização depende de como o Bitdefender é capaz de determiná-la:

- Caso o GPS esteja ativado no aparelho, sua localização pode ser determinada dentro de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o aparelho estiver dentro de casa, sua localização pode ser determinada em dezenas de metros caso o Wi-Fi esteja ativado e existam redes sem fio disponíveis no alcance.
- Caso contrário, a localização será determinada utilizando somente informações a partir da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Para se assegurar de que seu filho vai a certos locais, você pode criar uma lista de locais seguros e não seguros.

Para configurar um local:

1. Clique em **Dispositivos** na janela **Lugares**.
2. Clique em **ESCOLHER DISPOSITIVOS** e então selecione o dispositivo que você deseja configurar.
3. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
4. Escolha o tipo de local, **Seguro** ou **Restrito**.
5. Digite um nome válido para a área onde seu filho tem ou não permissão para ir.
6. Em **Lugar original**, digite a cidade onde seu filho deve estar e escolha o bairro da lista que aparecerá.
7. Defina a distância que deverá ser utilizada para monitoramento na barra **Raio**.
8. Clique em **ADICIONAR ÁREA** para salvar suas configurações.

25.3.6. Social

O Consultor Parental monitora a conta de seu filho no Facebook e relata as principais atividades que ocorrem.

Essas atividades online são verificadas e você receberá um aviso caso elas sejam ameaças à privacidade de seu filho.

Os elementos monitorados da conta online incluem:

- o número de amigos
- comentários do seu filho ou dos seus amigos nas suas fotos ou posts
- mensagens
- postagens no painel
- vídeos e fotos carregadas
- definições de privacidade da conta

Para configurar a proteção de Facebook para uma determinada conta de usuário:

1. Digite o e-mail da conta monitorada de seu filho e clique em **ENVIAR**.

   Informe seu filho de suas intenções, e peça a ele que clique no nosso link de ativação que ele recebeu por e-mail.

2. Para proteger a conta do Facebook da criança, ela deverá clicar no botão **INSTALAR APLICATIVO** que aparecerá assim que ela acessar sua conta do Facebook.

Para parar de monitorar a conta do Facebook, use o botão **Desvincular Conta** na parte superior.

26. USB IMMUNIZER

A funcionalidade Autorun embutida ao sistema operacional Windows é uma ferramenta bastante útil que permite aos computadores executarem automaticamente um arquivo de um dispositivo de mídia conectado a ele. Por exemplo, as instalações de software podem iniciar automaticamente quando o CD é inserido no drive de CD-ROM.

Infelizmente, esta funcionalidade também pode ser usada pelo malware para iniciar automaticamente e infiltrar no seu computador a partir de dispositivos media graváveis, tais como drives USB flash e cartões de memória conectados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB, você poderá evitar que qualquer drive flash formatado em NTFS, FAT32 ou FAT jamais possa executar malware automaticamente. Uma vez que um dispositivo USB esteja imunizado, o malware já não poderá configurá-lo para executar determinado aplicativo quando o dispositivo estiver conectado a um computador com Windows.

Para imunizar um dispositivo USB, siga estes passos:

1. Conecte o flash drive ao seu computador.
2. Explore o seu computador para localizar o dispositivo de armazenagem removível e clique com o botão direito do mouse sobre o mesmo.
3. No menu contextual, aponte para o **Bitdefender** e selecione **Imunizar este drive**.

Nota

Caso o drive já tenha sido imunizado, a mensagem **O dispositivo USB está protegido contra o malware baseado no autorun** aparecerá ao invés da opção Imunizar.

Para evitar que o seu computador execute malware de dispositivos USB não imunizados, desative a função de media autorun. Para mais informações, por favor consulte *"Usando o monitoramento automático de vulnerabilidade"* (p. 120).

OTIMIZAÇÃO DO SISTEMA

27. PERFIS

Atividades de trabalho diárias, assistir filmes ou jogar games podem causar lentidão no sistema, especialmente se eles estiverem sendo executados simultaneamente com os processos de atualização do Windows e tarefas de manutenção. Com o Bitdefender, você pode escolher e aplicar o seu perfil preferido; isso irá fazer ajustes no sistema para melhorar o desempenho de aplicativos específicos.

O Bitdefender fornece os seguintes perfis:

- Perfil de Trabalho
- Perfil de Filme
- Perfil de Jogo

Caso você decida não usar os **Perfis**, um perfil padrão chamado **Padrão** será ativado e ele não fará qualquer otimização no seu sistema.

De acordo com a sua atividade, as seguintes configurações do produto serão aplicadas quando um perfil é ativado:

- Todos os alertas e pop-ups do Bitdefender estão desativados.
- A Atualização Automática é adiada.
- As análises programadas são adiadas.
- O Consultor de Buscas é desabilitado.
- A Detecção de Invasão está configurada para o nível de proteção **Permissivo**.
- As ofertas especiais e as notificações de produto estão desativadas.

De acordo com a sua atividade, as seguintes configurações do sistema são aplicadas quando um perfil é ativado:

- A Atualização Automática do Windows é adiada.
- Alertas e pop-ups do Windows são desabilitados.
- Programas em segundo plano desnecessários são suspensos.
- Os efeitos visuais são ajustados para o melhor desempenho.
- Tarefas de manutenção são adiadas.
- A configuração do plano de energia é ajustada.

27.1. Perfil de Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com seus colegas distantes ou trabalhar com aplicativos de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi projetado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

Configurando o Perfil de Trabalho

Para definir as ações a serem tomadas durante o Perfil de Trabalho, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela de **Configurações de Perfil**, clique no botão **Configurar** na área do Perfil de Trabalho.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos aplicativos de trabalho
   - Otimize as configurações do produto para perfil de Trabalho
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
6. Clique **Salvar** para salvar as alterações e fechar a janela.

Adicionar aplicativos manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando você abrir um determinado aplicativo de trabalho, você pode adicionar o aplicativo manualmente à **Lista de Aplicativos**.

Para adicionar aplicativos manualmente à Lista de aplicativos do Perfil de Trabalho:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois clique no botão **Configurar** na área de perfil de Trabalho.
4. Na janela do **Perfil de Trabalho**, clique no link **Lista de aplicativos**.
5. Clique em **Adicionar** para adicionar um novo aplicativo à **Lista de aplicativos**.

   Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.

27.2. Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as configurações de sistema e do produto para que você possa desfrutar de uma experiência cinematográfica agradável e sem interrupção.

Configurando o Perfil de Filme

Para definir as ações a serem tomadas no Perfil de Filme:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Configurações de Perfis**, clique no botão **Configurar** na área do Perfil de Filme.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos reprodutores de vídeo
   - Otimize as configurações do produto para Perfil de filme
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajustar configs do plano de energia para Modo Filme.

6. Clique **Salvar** para salvar as alterações e fechar a janela.

Adicionando manualmente reprodutores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Filme ao iniciar um determinado aplicativo de reprodução de vídeo, você pode adicionar manualmente o aplicativo à **Lista de reprodutores**.

Para adicionar manualmente reprodutores de vídeo à Lista de reprodutores no Perfil de Filme:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois clique no botão **Configurar** na área de perfil de Filme.
4. Na janela **Perfil de Filme**, clique no link **Lista de reprodutores**.
5. Clique em **Adicionar** para adicionar um novo aplicativo à **Lista de reprodutores**.

   Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.

27.3. Perfil de Jogo

Para desfrutar de uma experiência de jogo ininterrupta é importante reduzir interrupções do sistema e diminuir a lentidão. Usando heurísticas comportamentais, juntamente com uma lista de jogos conhecidos, o Bitdefender pode detectar automaticamente os jogos em execução e otimizar os recursos do sistema para que você possa aproveitar a sua pausa para jogo.

Configurando o Perfil de Jogo

Para definir as ações a serem tomadas durante o perfil de jogo, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.

3. Clique no módulo de **Perfis**.
4. Na janela **Configurações de Perfis**, clique no botão **Configurar** na área do Perfil de Jogo.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho nos jogos
   - Otimize as configurações do produto para Perfil de jogo
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajustar configs do plano de energia para Modo Jogo.
6. Clique **Salvar** para salvar as alterações e fechar a janela.

Adicionando jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo ao iniciar um determinado jogo ou aplicativo, você pode adicionar o aplicativo à **Lista de jogos** manualmente.

Para adicionar manualmente jogos à Lista de jogos no Perfil de Jogo:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois clique no botão **Configurar** na área de perfil de Jogos.
4. Na janela **Perfil de Jogo**, clique no link **Lista de jogos**.
5. Clique em **Adicionar** para adicionar um novo jogo à **Lista de jogos**.

   Uma nova janela aparece. Vá até o arquivo executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

27.4. Otimização em Tempo Real

A Otimização em Tempo Real do Bitdefender é um plug-in que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que você não seja interrompido enquanto está em um modo de perfil. Dependendo da carga do CPU, o plug-in monitora todos os processos,

focando naqueles que usam uma carga maior, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Ferramentas**.
3. Clique no módulo **Perfis**, depois selecione a aba **Configurações de Perfis**.
4. Ative ou desative a Otimização em Tempo Real automática clicando no botão correspondente.

28. RESOLVENDO INCIDÊNCIAS COMUNS

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o Bitdefender e as possíveis soluções. A maioria destes problemas pode ser resolvida com a configuração correcta das definições do produto.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo “*Solicite Ajuda*” (p. 201).

28.1. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Caso note uma diminuição de velocidade significativa, este problema pode ocorrer pelos seguintes motivos:

- **O Bitdefender não é o único programa de segurança instalada no sistema.**

  Apesar de o Bitdefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todos os

outros programas antivírus utilizados antes de instalar o Bitdefender. Para mais informações, por favor consulte *"Como posso remover outras soluções de segurança?"* (p. 76).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o Bitdefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver executando multiplos aplicativos ao mesmo tempo. Para mais informações, por favor consulte *"Requisitos mínimos do sistema"* (p. 3).

- **Você instalou aplicativos que não utiliza**.

  Qualquer computador possui programas ou aplicativos que você não utiliza. E quaisquer programas indesejados são executados no plano de fundo, ocupando espaço no disco rígido e memória. Caso não utilize um programa, desinstale-o. Isso também se aplica a qualquer outro programa pré-instalado ou aplicativo de teste que tenha esquecido de remover.

Importante

Caso suspeite que um programa ou aplicativo seja parte essencial de seu sistema operacional, não remova o mesmo e entre em contato com a Assistência ao Cliente Bitdefender para assistência.

- **Seu sistema pode estar infectado**.

  A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelo malware. Spyware, viruses, Trojans e adware prejudicam o desempenho de seu sistema. Certifique-se de analisar o seu sistema periodicamente, pelo menos uma vez por semana. Recomendamos utilizar a Verificação de Sistema do Bitdefender pois a mesma verifica todos os tipos de malware que estejam ameaçando a segurança do seu sistema.

  Para iniciar a Análise do Sistema, siga estes passos:

  1. Clique no ícone no canto inferior direito da interface do Bitdefender.
  2. Selecione a aba **Proteção**.
  3. No módulo **Antivírus**, selecione a **Análise de Sistema**.
  4. Siga os passos do assistente.

28.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do Bitdefender que não foi totalmente removida ou uma instalação do Bitdefender mal sucedida.**

  Neste caso, siga os passos seguintes:

  1. Remover o Bitdefender totalmente do sistema:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
       d. Clique em **Próximo** para continuar.
       e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
     - No **Windows 8 e Windows 8.1**:
       a. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
       c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
       d. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
       e. Clique em **Próximo** para continuar.
       f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
     - No **Windows 10**:
       a. Clique em **Iniciar** e depois em Configurações.

b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.

c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar sua escolha.

e. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.

f. Clique em **Próximo** para continuar.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

2. Reinstale seu produto Bitdefender

- **O Bitdefender não é a única solução de segurança instalada no seu sistema.**

Neste caso, siga os passos seguintes:

1. Remover a outra solução de segurança. Para mais informações, por favor consulte *"Como posso remover outras soluções de segurança?"* (p. 76).
2. Remover o Bitdefender totalmente do sistema:

- No **Windows 7**:

a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.

b. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.

c. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.

d. Clique em **Próximo** para continuar.

e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 8 e Windows 8.1**:

a. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.

e. Clique em **Próximo** para continuar.

f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 10**:

a. Clique em **Iniciar** e depois em Configurações.

b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.

c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar sua escolha.

e. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.

f. Clique em **Próximo** para continuar.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

3. Reinstale seu produto Bitdefender

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 201).

28.3. Já não consigo utilizar um aplicativo

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Após instalar o Bitdefender você poderá se deparar com uma das seguintes situações:

- Poderá receber uma mensagem do Bitdefender a informar que o programa está a tentar modificar o sistema.

- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o Controle Ativo de Ameaças detecta erroneamente que alguns aplicativos são maliciosos.

O Controle Ativo de Ameaças é um módulo do Bitdefender que monitora constantemente os aplicativos executados em seu sistema e reporta aqueles com comportamento potencialmente malicioso. Já que esta função é baseada em um sistema heurístico, pode haver casos em que aplicativos legítimos sejam reportados pelo Controle Ativo de Ameaças.

Quando essa situação ocorrer, você poderá excluir o aplicativo respectivo da monitoração do Controle de Ameaças Ativas.

Para adicionar o programa à lista de exclusões, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Antivírus**, depois selecione a aba **Exclusões**
4. Clique no link **Processos Excluídos**. Na janela que aparece, você pode gerenciar as exclusões de processos do Controle Ativo de Ameaças.
5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione o aplicativo que quer excluir e depois clique em **OK**.
   c. Mantenha a opção **Permitir** selecionada para prevenir que o Controle Ativo de Ameaças bloqueie o aplicativo.
   d. Clicando **Adicionar**.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 201).

28.4. O que fazer quando o Bitdefender bloqueia um website ou um aplicativo online seguro

O Bitdefender oferece uma experiência de navegação de rede segura filtrando todo o tráfego da rede e bloqueando conteúdos maliciosos. No entanto, é

possível que o Bitdefender considere um website ou um aplicativo online seguro como inseguro, o que fará que a análise de tráfego de HTTP do Bitdefender bloqueie-os incorretamente.

Se a mesma página ou aplicativo for bloqueado repetidamente, eles podem ser adicionados a uma lista segura para que não sejam analisados pelos mecanismos do Bitdefender, assegurando uma experiência de navegação da rede normal.

Para adicionar um website na **Lista segura**, sigas esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Proteção da Internet**.
4. Na aba **Configurações**, clique no link **Lista segura**.
5. Forneça o endereço do website ou do aplicativo online bloqueado no campo correspondente e clique em **Adicionar**.
6. Clique **Salvar** para salvar as alterações e fechar a janela.

Apenas os websites e aplicativos que você confia completamente devem ser adicionados a essa lista. Esses serão excluídos da análise pelos seguintes mecanismos: malware, phishing e fraude.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 201).

28.5. Não consigo conectar-me à Internet

Poderá verificar que um programa ou navegador da rede já não consegue conectar-se à Internet ou acessar os serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente conexões de e para o respectivo aplicativo de software.

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall** e então selecione a aba **Regras**.
4. Para adicionar uma regra de aplicativo, clique no botão **Adicionar regra**.

5. Uma nova janela aparecerá para que você possa inserir as informações. Certifique-se de selecionar todos os tipos de rede disponíveis e na seção **Permissão** selecionar **Permitir**.

Feche o Bitdefender, abra o aplicativo de software e tente conectar-se à Internet novamente.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 201).

28.6. Não consigo acessar um dispositivo na minha rede

Dependendo da rede a que está conectado, a firewall do Bitdefender poderá bloquear a conexão entre o seu sistema e outro dispositivo (como outro computador ou uma impressora). Como resultado, já não poderá partilhar ou imprimir arquivos.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente conexões de e para o respectivo dispositivo. Para cada conexão de rede você pode configurar uma zona confiável e especial.

Uma zona confiável é um dispositivo em que você confia plenamente. Todo o tráfego entre o seu computador e o dispositivo confiável é permitido. Para partilhar recursos com dispositivos específicos, tais como computadores ou impressoras, adicione-as como zonas confiáveis.

Para adicionar uma zona confiável em seus adaptadores de rede, siga estas etapas:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. Clique no módulo **Firewall** e então selecione a aba **Regras**.
4. Para adicionar uma zona, clique no botão **Adicionar regra**. Surgirá uma nova janela apresentando os endereços IP dos dispositivos ligados à rede.
5. Selecione o endereço IP do computador ou a impressora que deseja adicionar, ou digite um endereço ou intervalo de endereço na caixa de texto fornecida.
6. No campo **Permissão** selecione **Permitir** e depois clique em **OK**.

Se você ainda não consegue se conectar ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Verifique a existência de outras causas potenciais, tais como as seguintes:

- A firewall no outro computador poderá bloquear a partilha de arquivos e impressoras com o seu computador.
  - Se o Firewall do Windows for usado, pode ser configurado para compartilhar arquivos e impressoras da seguinte forma:
    - No **Windows 7**:
      1. Clique em **Iniciar**, vá ao **Painel de Controle** e selecione **Sistema e Segurança**.
      2. Acesse **Windows Firewall** e clique em **Permitir um programa através do Windows Firewall**.
      3. Selecione a caixa de marcação **Compartilhar Arquivos e Impressoras**.
    - No **Windows 8 e Windows 8.1**:
      1. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
      2. Clique em **Sistema e Segurança**, acesse **Windows Firewall** e selecione **Permitir um aplicativo através do Windows Firewall**.
      3. Selecione a caixa de seleção **Compartilhamento de Arquivos e Impressoras** e clique em **OK**.
    - No **Windows 10**:
      1. Digite "Permitir um aplicativo através do Firewall do Windows" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente.
      2. Clique em **Alterar configurações**.
      3. Na lista **Aplicativos e recursos permitidos**, selecione a caixa de seleção **Compartilhamento de Arquivos e Impressoras** e clique em **OK**.
  - Se outro programa de firewall é usado, por favor consulte a sua documentação ou o arquivo de ajuda.

- Condições gerais que podem impedir ou uso ou a conexão com a impressora compartilhada:
  - Você pode precisar fazer logon em uma conta administrador do Windows para acessar a impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso apenas para usuários e computadores específicos. Se você está compartilhando a sua impressora, verifique as permissões definidas para a impressora para ver se o usuário do outro computador é permitido o acesso à impressora. Se você está tentando se conectar a uma impressora compartilhada, verifique com o usuário no outro computador, se você tem permissão para se conectar à impressora.
  - A impressora conectada ao seu computador ou a outro computador não está compartilhada.
  - A impressora compartilhada não é adicionada no computador.

  > **Nota**
  > Para aprender como gerenciar o compartilhamento de impressora (compartilhar uma impressora, definir ou remover permissões para uma impressora, conectar-se a uma impressora da rede, ou a uma impressora compartilhada), vá para a Ajuda do Windows e Centro de Suporte (no menu Iniciar, clique **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restrito a computadores ou usuários específicos. Você deve verificar com o administrador da rede se possui ou não permissão para acessar a impressora.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 201).

28.7. A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para resolver esta situação, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.

3. Clique no módulo **Firewall** e então clique na chave para desativar o **Firewall**.
4. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.
   - Caso você ainda com uma conexão lenta à Internet, a incidência poderá não ser causada pelo Bitdefender. Você deve contatar o seu Provedor de Serviços de Internet para confirmar se a conexão está operacional.

     Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção "*Solicite Ajuda*" (p. 201).
   - Se a conexão com a Internet melhorou depois de desativar a firewall do Bitdefender, siga estes passos:
     a. Clique no ícone no canto inferior direito da interface do Bitdefender.
     b. Selecione a aba **Proteção**.
     c. Clique no módulo **Firewall** e então selecione a aba **Configurações**.
     d. Acesse **Bloquear scans de portas na rede** e clique no botão para ativá-lo.
     e. Acesse a aba **Adaptadores** e selecione sua conexão de Internet.
     f. Na coluna **Tipo de Rede** selecione **Casa/Trabalho**.
     g. Na coluna **Modo Invisível**, selecione **LIGADO**. Configure a coluna **Genérico** como **Ativado**
     h. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de conexão à Internet.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 201).

28.8. Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.

Para manter o seu sistema atualizado com as mais recentes assinaturas de malware Bitdefender, siga os seguintes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Configurações Gerais** no menu suspenso.
2. Na janela de **Configurações Gerais**, selecione a aba **Atualizar**.
3. Próximo a **Atualizar as regras de processamento**, selecione **Exibir antes de fazer download** do menu suspenso.
4. Volte à janela principal e clique no botão de ação **Atualizar** na interface do Bitdefender.
5. Selecione apenas **Atualizações das assinaturas** e clique em **OK**.
6. O Bitdefender vai transferir e instalar apenas as atualizações das assinaturas de malware.

28.9. O meu computador não está conectado à Internet. Como eu posso atualizar o Bitdefender?

Se o seu computador não estiver ligado à Internet, tem de transferir manualmente as atualizações para um computador com acesso à Internet e, depois, transferi-las para o seu computador com um dispositivo amovível, por exemplo, um USB.

Siga esses passos:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. Na coluna **Atualização Manual**, clique na hiperligação que corresponde ao seu produto e à arquitectura do sistema. Se não sabe se a versão do seu Windows é de 32 ou 64 bits, consulte *"Estou usando uma versão de 32 ou 64 Bit do Windows?"* (p. 75).
3. Guarde o arquivo com o nome weekly.exe no sistema.
4. Mova o arquivo transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no arquivo e siga os passos do assistente.

28.10. Os Serviços do Bitdefender não estão respondendo

Este artigo ajuda você a solucionar o erro **Os Serviços do Bitdefender não estão respondendo**. Você pode encontrar esse erro da seguinte forma:

- O ícone do Bitdefender na bandeja do sistema está cinza e você recebe a informação de que os serviços do Bitdefender não estão respondendo.
- A janela do Bitdefender mostra que os serviços do Bitdefender não estão respondendo.

O erro pode ser causado por uma das seguintes condições:

- Erro temporário de comunicação entre os serviços do Bitdefender.
- Alguns dos serviços do Bitdefender estão parados.
- outras soluções de segurança sendo executadas em seu computador ao mesmo tempo com o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere um pouco e veja se alguma coisa muda. O erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até que o Bitdefender seja carregado. Abra o Bitdefender para verificar se o erro persiste. Reiniciar o computador normalmente resolve o problema.
3. Verifique se há alguma outra solução de segurança instalada, pois ela poderão afetar o funcionamento do Bitdefender. Se este for o caso, recomendamos que você remova todas as outras soluções de segurança e então reinstale o Bitdefender.

   Para mais informações, por favor consulte "*Como posso remover outras soluções de segurança?*" (p. 76).

Se o erro persistir, entre em contato com nossos representantes de suporte conforme descrito na seção "*Solicite Ajuda*" (p. 201).

28.11. O filtro antispam não funciona corretamente

Este artigo ajuda você solucionar os seguintes problemas relacionados com as operações de filtragem do Bitdefender Antispam:

- Um número de mensagens de e-mail legítimas estão marcados como [spam].

- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não detecta qualquer mensagem de Spam.

28.11.1. Mensagens legítimas são marcadas como [spam]

Valida mensagens que estão marcadas como [spam] simplesmente porque elas parecem como spam para o filtro antispam Bitdefender. Normalmente, você pode resolver este problema ao configurar adequadamente o filtro antispam.

Bitdefender adiciona automaticamente os destinatários de suas mensagens de e-mail à sua lista de Amigos. As mensagens de e-mail recebidas de contatos na lista de Amigos, são consideradas legítimas. Elas não são verificadas pelo filtro antispam, e portanto, nunca são marcadas como [spam].

A configuração automática da lista de Amigos, não previne a detecção de erros que possam ocorrer nestas situações:

- Você recebe uma grande quantidade de e-mails com fins comerciais, como resultado de ter se registrado em vários sites. Neste caso, a solução é adicionar o endereço de e-mail de onde você recebe tais mensagens à lista de Amigos.
- Uma parte significante de seus e-mails legítimos vem de pessoas das quais você nunca trocou e-mail antes, tal como clientes, potenciais sócios de negócios e outros. Outra solução é necessária neste caso.

  Se estiver usando um cliente de e-mail com o qual o Bitdefender é compatível, indique erros de detecção.

Nota
O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para *"Clientes de e-mail e protocolos suportados"* (p. 107).

Adicionar contatos à Lista de Amigos

Se você está usando um cliente de e-mail suportado, você pode facilmente adicionar os remetentes de mensagens legítimas à lista de Amigos. Siga esses passos:

1. Em seu cliente de e-mail, selecione uma mensagem de e-mail do remetente que você deseja adicionar à lista de Amigos.
2. Clique o botão **Adicionar Amigo** à barra de ferramentas do antispam do Bitdefender.
3. Poderá lhe ser solicitado a acusar o recebimento do endereço adicionado à lista de Amigos. Selecione **Não mostre esta mensagem novamente** e clique **OK**.

Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.

Se você está usando um cliente de e-mail diferente, você pode adicionar contatos à lista de Amigos da interface do Bitdefender. Siga esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antispam**, selecione **Gerenciar Amigos**.

   Uma janela de confirmação aparecerá.
4. Digite o endereço de e-mail onde deseja sempre receber as mensagens de e-mail e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

Indica os erros de detecção

Se você está usando um cliente de e-mail suportado, você pode facilmente corrigir o filtro antispam (indicando qual mensagem de e-mail não deve ser marcada como [spam]). Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique o botão **Adicionar Amigos** na barra de ferramentas do antispam do Bitdefender para adicionar o remetente à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.

5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). A mensagem de e-mail será removida para a pasta de Entrada.

28.11.2. Muitas mensagens de spam não são detetadas

Se você está recebendo muitas mensagens que não estão marcadas como [spam], você precisa configurar o filtro antispam do Bitdefender para poder melhorar sua eficiência.

Tente as seguintes soluções:

1. Se estiver usando um cliente de e-mail com o qual o Bitdefender é compatível, indique mensagens de spam não detectadas.

Nota

O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para *"Clientes de e-mail e protocolos suportados"* (p. 107).

2. Adicionar spammers à lista de Spammers. As mensagens de e-mail recebidas destes endereços na lista de Spammers, são automaticamente marcados como [spam].

Indica mensagens de spam não detectadas

Se você está usando um cliente de e-mail suportado, você pode facilmente indicar quais mensagens de e-mail foram detectadas como spam. Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a Pasta de Entrada.
3. Selecione as mensagens spam não detectadas.
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). Elas são marcadas imediatamente como [spam] e movidas para a pasta lixo.

Adicionar spammers à Lista de Spammers.

Se você está usando um cliente de e-mail suportado, você pode fácilmente adicionar os remetentes das mensagens de spam, à lista de Spammers. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione as mensagens marcadas como [spam] pelo Bitdefender.
4. Clique o botão **Adicionar Spammer** na barra de ferramentas do antispam do Bitdefender.
5. Lhe poderá ser solicitado acusar recebimento do endereço adicionado à lista de Spammers. Selecione **Não mostre esta mensagem novamente** e clique **OK**.

Caso esteja usando um cliente de e-mail diferente, você pode adicionar spammers manualmente à lista de Spammers da interface do Bitdefender. É conveniente fazer isto somente quando você recebe várias mensagens spam do mesmo endereço de e-mail. Siga esses passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antispam**, selecione **Gerenciar Spammers**.

   Uma janela de confirmação aparecerá.
4. Digite o endereço de e-mail do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

28.11.3. O filtro antispam não detecta nenhuma mensagem spam

Se nenhuma mensagem de spam for marcada como [spam], poderá haver um problema com o filtro antispam do Bitdefender. Antes de resolver este problema, certifique-se de que não é causado por uma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o status da proteção antispam, clique na seta no canto inferior esquerdo da interface

do Bitdefender, selecione a aba **Proteção**, clique no módulo **Antispam** e ative o botão na janela **Configurações**.

Se o Antispam estiver desligado, é isso que está causando o problema. Clique no botão para ligar a proteção antispam.

- A proteção Antispam do Bitdefender está disponível apenas para clientes de correio eletrônico configurado para receber mensagens de e-mail via protocolo POP3. Isso significa o seguinte:
  - E-mails recebidos através de serviços e-mail baseados em web (tais como Yahoo, Gmail, Hotmail ou outro) não são filtrados por envio de spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo além de POP3 (por exemplo, IMAP4), o filtro Antispam do Bitdefender não os verifica por envio de spam.

Nota

POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, pergunte à pessoa que configurou o seu cliente de e-mail.

- Bitdefender Internet Security 2016 não verifica tráfego POP3 do Lotus Notes.

Uma possível solução é reparar ou reinstalar o produto. Contudo, você poderá contatar a Bitdefender para suporte, como descrito na seção *“Solicite Ajuda”* (p. 201).

28.12. A funcionalidade Preenchimento Automático não funciona na minha Carteira

Você salvou suas credenciais online na Carteira do Bitdefender e constatou que o preenchimento automático não está funcionando. Normalmente esse problema aparece quando a extensão do Gerenciador de Senhas do Bitdefender não está instalada em seu computador.

Para resolver esta situação, siga os seguintes passos:

- No **Internet Explorer:**

  1. Abra o Internet Explorer.

2. Clique em Ferramentas.
3. Clique em Gerenciar Suplementos.
4. Clique em Barras de Ferramentas e Extensões.
5. Selecione o **Bitdefender Gerenciador de Senhas** e clique em Ativar.

- No **Mozilla Firefox:**
  1. Abrir o Mozilla Firefox.
  2. Clique em Ferramentas.
  3. Clique em Add-ons.
  4. Clique em Extensões.
  5. Selecione o **Bitdefender Gerenciador de Senhas** e clique em Ativar.
- No **Google Chrome:**
  1. Abrir o Google Chrome.
  2. Acesse o ícone Menu.
  3. Clique em Definições.
  4. Clique em Extensões.
  5. Selecione o **Bitdefender Gerenciador de Senhas** e clique em Ativar.

Nota

O add-on será ativado após você reiniciar seu navegador.

Agora verifique se o recurso de auto completar na Carteira está funcionando para suas contas online.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 201).

28.13. A Remoção do Bitdefender falhou

Caso queira remover o seu produto Bitdefender e observar que o processo demora ou o sistema trava, clique em **Cancelar** para abortar a ação. Caso não funcione, reinicie o sistema.

Se a remoção falhar, algumas chaves do registro e arquivos do Bitdefender poderão permanecer em seu sistema. Estes arquivos remanescentes poderão

evitar uma nova instalação do Bitdefender. Elas também podem afetar o desempenho do sistema e sua estabilidade.

Para remover completamente Bitdefender do seu sistema, siga estes passos:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  3. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo**.
  4. Clique em **Próximo** para continuar.
  5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 8 e Windows 8.1**:
  1. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo**.
  5. Clique em **Próximo** para continuar.
  6. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
  1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  3. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar.**
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Clique em **Remover**. Logo, selecione **Quero reinstalá-lo.**
  6. Clique em **Próximo** para continuar.

7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

28.14. O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, são vários os motivos para este tipo de problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

  Para resolver isto, siga estes passos:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte *"Como posso reiniciar no Modo de Segurança?"* (p. 77).
  2. Remove Bitdefender do seu sistema:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
       d. Clique em **Próximo** para continuar.
       e. Aguarde até que o processo de desinstalação seja finalizado.
       f. Reinicie seu sistema no modo normal.
     - No **Windows 8 e Windows 8.1**:
       a. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
d. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
e. Clique em **Próximo** para continuar.
f. Aguarde até que o processo de desinstalação seja finalizado.
g. Reinicie seu sistema no modo normal.

- No **Windows 10**:

a. Clique em **Iniciar** e depois em Configurações.
b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
c. Encontre o **Bitdefender Internet Security 2016** e selecione **Desinstalar**.
d. Clique em **Desinstalar** novamente para confirmar sua escolha.
e. Clique em **Remover** na janela que aparece e depois selecione **Quero reinstalá-lo**.
f. Clique em **Próximo** para continuar.
g. Aguarde até que o processo de desinstalação seja finalizado.
h. Reinicie seu sistema no modo normal.

3. Reinstale seu produto Bitdefender

- **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**

Para resolver isto, siga estes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte *"Como posso reiniciar no Modo de Segurança?"* (p. 77).
2. Remova as demais soluções de segurança do seu sistema:

- No **Windows 7**:

a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.

b. Encontre o nome do programa que pretende remover e selecione **Remover**.

c. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 8 e Windows 8.1**:

  a. A partir da tela Iniciar do Windows, localize **Painel de Controle** (por exemplo, você pode começar a digitar "Painel de Controle" diretamente no menu Iniciar) e então clicar em seu ícone.

  b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

  c. Encontre o nome do programa que pretende remover e selecione **Remover**.

  d. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

- No **Windows 10**:

  a. Clique em **Iniciar** e depois em Configurações.

  b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.

  c. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.

  d. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

Para desinstalar corretamente outro software, acesse o site do fornecedor e execute a ferramenta de desinstalação ou contate-o diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

Já seguiu os passos acima e o problema não está resolvido.

Para resolver isto, siga estes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte *"Como posso reiniciar no Modo de Segurança?"* (p. 77).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.

3. Reinicie o sistema no modo normal e contate os nossos representantes do suporte conforme descrito na seção “*Solicite Ajuda*” (p. 201).

29. REMOVER MALWARE DO SEU SISTEMA

O malware pode afectar o seu sistema de várias formas e a actuação do Bitdefender depende do tipo de ataque por malware. Como os vírus alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

Há situações em que o Bitdefender não consegue remover automaticamente a infecção por malware do seu sistema. Nestes casos, a sua intervenção é necessária.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo *"Solicite Ajuda"* (p. 201).

29.1. Modo de Recuperação Bitdefender

Modo do Recuperação é uma característica do Bitdefender que lhe permite analisar e desinfectar todas as partições do disco rígido existentes fora do seu sistema operacional.

Depois de instalar o Bitdefender Internet Security 2016, o Modo de Recuperação pode ser usado mesmo que você não consiga inicialiar no Windows.

Iniciar o seu sistema no Modo de Recuperação

Você pode entrar no Modo de Recuperação de duas formas:

Na interface do Bitdefender

Para entrar no Modo de Recuperação diretamente a partir do Bitdefender, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione a aba **Proteção**.
3. No módulo **Antivírus**, selecione **Modo de Recuperação**.

   Uma janela de confirmação aparecerá. Clique **Sim** para reiniciar o seu computador.
4. Após a reinicialização do computador, aparecerá um menu solicitando que você selecione um sistema operacional. Escolha **Modo de Recuperação do Bitdefender** e pressione **Enter** para iniciar no ambiente do Bitdefender, de onde você pode limpar a sua partição do Windows.
5. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa. Depois pressione novamente **Enter**.

   O Modo de Recuperação do Bitdefender irá carregar dentro de alguns minutos.

Inicialize o seu computador diretamente no Modo de Recuperação

Se o Windows já não iniciar, você pode inicializar o seu computador diretamente no Modo de Recuperação do Bitdefender, seguindo os passos abaixo:

1. Inicie / reinicie o seu computador e comece a pressionar a tecla **espaços** do seu teclado antes de aparecer o logo do Windows.
2. Um menu aparecerá solicitando que você selecione um sistema operacional para iniciar. Pressione **TAB** para ir para a área de ferramentas. Escolha **Imagem de Recuperação Bitdefender** e prima a tecla **Enter** inicializar num ambiente do Bitdefender onde poderá limpar a sua partição Windows.

3. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa. Depois pressione novamente **Enter**.

   O Modo de Recuperação do Bitdefender irá carregar dentro de alguns minutos.

Analisar o seu sistema no Modo de Recuperação

Para analisar o seu sistema no Modo de Recuperação, siga os seguintes passos:

1. Entre no Modo de Recuperação, conforme descrito em "Iniciar o seu sistema no Modo de Recuperação" (p. 192).
2. O logo do Bitdefender surgirá e os motores antivírus começarão a ser copiados.
3. Uma janela de boas-vindas aparecerá. Clique em **Continuar**.
4. Iniciou-se uma atualização de assinaturas antivirus.
5. Após o fim da atualização, a janela do Verificador de Antivírus do Bitdefender aparecerá.
6. Clique em **Analisar Agora**, selecione o alvo da análise na janela que surge e clique em **Abrir** para iniciar a análise.

   Recomenda-se que analise toda a partição do Windows.

Nota

Ao trabalhar no Modo de Recuperação, você lida com nomes de partições do tipo do Linux. As partições do disco surgirão como sda1 provavelmente correspondendo à (C:) partição do Windows, sda2 correspondendo a (D:) e assim sucessivamente.

7. Aguarde o término da análise. Caso algum malware seja detectado, siga as instruções para remover a ameaça.
8. Para sair do Modo de Recuperação, clique com o botão direito do mouse numa área vazia da Área de Trabalho, selecione **Sair** no menu que aparece e depois escolha entre reiniciar ou encerrar o computador.

29.2. O que fazer se o Bitdefender encontrar vírus no seu computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O Bitdefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o Bitdefender bloqueou um ou vários vírus no seu computador.

Nestas situações, atualize o Bitdefender para se certificar que possui as assinaturas de malware mais recentes e realize uma Análise de Sistema.

Assim que a análise terminar, selecione a ação pretendida para os itens infectados (Desinfectar, Eliminar, Mover para a Quarentena).

Atenção

Se suspeitar que o arquivo faz parte do sistema operativo do Windows ou que não é um arquivo infectado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efectuar a ação seleccionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) arquivo(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone no canto inferior direito da interface do Bitdefender.
   b. Selecione a aba **Proteção**.
   c. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
   d. Clique no botão para desligar **Análise no-acesso**.
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte *“Como posso mostrar objetos ocultos no Windows?”* (p. 75).
3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
4. Active a proteção antivírus em tempo real do Bitdefender.

No caso de o primeiro método falhar ao remover a infecção, siga os seguintes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte *"Como posso reiniciar no Modo de Segurança?"* (p. 77).
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte *"Como posso mostrar objetos ocultos no Windows?"* (p. 75).
3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 201).

29.3. Como posso limpar um vírus num arquivo?

Um arquivo é um arquivo ou um conjunto de arquivos comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os arquivos.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detectar a presença de vírus no interior, mas não pode aplicar outras ações.

Se o Bitdefender avisar que foi detectado um vírus dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover o vírus devido a restrições nas definições de permissão do arquivo.

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o arquivo que contém o vírus ao realizar uma Análise Completa do sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone no canto inferior direito da interface do Bitdefender.
   b. Selecione a aba **Proteção**.

c. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.
   d. Clique no botão para desligar **Análise no-acesso**.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o arquivo infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os arquivos num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma análise completa ao sistema para se certificar que não há outras infecções no sistema.

Nota
É importante observar que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema, pois o vírus deve ser descompactado e executado para infectar o seu sistema.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 201).

29.4. Como posso limpar um vírus de um arquivo de correio eletrônico?

O Bitdefender também pode identificar vírus em bases de dados de correio eletrônico e arquivos de correio eletrônico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Pode limpar um vírus armazenado num arquivo de correio eletrônico da seguinte forma:

1. Analisar a base de dados do correio eletrônico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone no canto inferior direito da interface do Bitdefender.
   b. Selecione a aba **Proteção**.

c. Clique no módulo **Antivírus**, depois selecione a aba **Shield**.

d. Clique no botão para desligar **Análise no-acesso**.

3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio eletrônico.
4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrônico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Outlook Express: No menu Arquivo, clique em Pasta e, depois em Compactar Todas as Pastas.
   - No Microsoft Outlook 2007: No menu Arquivo, clique em Gestão de Arquivos de Dados. Selecione os arquivos das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
   - No Microsoft Outlook 2010 / 2013: No menu Arquivo, clique em Info e então em Configurações da Conta (Adicionar e remover contas ou alterar configurações de conexão existentes). Clique em Arquivo de Dados, selecione os arquivos das pastas (.pst) que pretende compactar e clique em Configurações. Clique em Compactar Agora.
6. Active a proteção antivírus em tempo real do Bitdefender.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 201).

29.5. O que fazer se eu suspeitar que um arquivo seja perigoso?

Você pode suspeitar que um arquivo do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detectado.

Para se certificar de que o seu sistema está protegido, siga estes passos:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como fazer isto, consulte “*Como posso analisar o meu sistema?*” (p. 58).

2. Se o resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o arquivo, entre em contato com os representantes do suporte para que possamos ajudá-lo.

   Para saber como fazer isto, consulte “*Solicite Ajuda*” (p. 201).

29.6. O que são arquivos protegidos por senha no registro de análise?

Isto é apenas uma notificação que indica que o Bitdefender detectou que estes arquivos estão protegidos por senha ou por outra forma de encriptação.

Normalmente, os itens protegidos por senha são:

- Arquivos que pertencem a outras solução de segurança.
- Arquivos que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes arquivos têm de ser extraídos ou de outra forma descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido. Se pretende analisar esses arquivos com Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses arquivos.

Recomendamos que ignore estes arquivos pois não constituem uma ameaça ao seu sistema.

29.7. Quais são os itens ignorados no relatório de análise?

Todos os arquivos que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa arquivos que não tenham sido alterados desde a última análise.

29.8. O que são arquivos muito comprimidos no registro de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria muito tempo, tornando o sistema instável.

Supercompactado significa que o Bitdefender não realizou a análise desse arquivo, pois a descompactação iria consumir muitos recursos do sistema. O conteúdo será analisado em acesso de tempo real, caso necessário.

29.9. Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?

Se for detectado um arquivo infectado, o Bitdefender tentará automaticamente desinfectá-lo. Se a desinfecção falhar, o arquivo é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

Este é, normalmente, o caso de arquivos de instalação que são transferidos de sítios de Internet suspeitos. Se se encontrar numa situação assim, transfira o arquivo de instalação do sítio de Internet do fabricante ou de outro sítio fiável.

30. SOLICITE AJUDA

A Bitdefender fornece aos seus clientes um nível de suporte rápido e eficaz. Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto Bitdefender, pode utilizar vários recursos em linha para encontrar uma solução ou resposta. Ou, se preferir você poderá contatar a equipe de Suporte ao Cliente Bitdefender. Os nossos técnicos de suporte responderão imediatamente às suas questões e proporcionarão a ajuda que precisar.

A seção "*Resolvendo incidências comuns*" (p. 167) fornece as informações necessárias em relação às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a resposta para sua pergunta nos recursos disponibilizados, pode contactar-nos diretamente:

- "Contacte-nos diretamente do seu produto Bitdefender" (p. 201)
- "Contate-nos através do nosso Centro de Suporte Online" (p. 202)

Contacte-nos diretamente do seu produto Bitdefender

Se possuir uma conexão ativa com a Internet, você pode entrar em contato com o suporte do Bitdefender diretamente da interface do produto.

Siga esses passos:

1. Clique no ícone no topo da interface do Bitdefender e selecione **Ajuda e Suporte** na lista de opções.
2. Você tem as seguintes opções:
   - **Documentação do Produto**

     Acesse nossa base de dados e procure a informação necessária.
   - **Contato com o Suporte**

     Use o botão **Contato com o Suporte** para executar a Ferramenta de Suporte do Bitdefender e contatar o Departamento de Suporte ao Cliente. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

     a. Selecione a caixa de verificação para indicar aceitação e clique em **Seguinte**.

     b. Complete o formulário de envio com os dados necessários:

i. Insira o seu endereço de e-mail.

ii. Digite o seu nome completo.

iii. Introduza a descrição do problema que encontrou.

iv. Marque a opção **Tentar reproduzir a incidência antes de enviar** caso você encontre uma incidência de produto. Continue com os passos necessários.

c. Por favor, aguarde alguns minutos enquanto o Bitdefender recolhe as informações relacionadas ao produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

d. Clique em **Concluir** para enviar as informações ao Departamento de Suporte ao Cliente Bitdefender. Você será contactado assim que possível.

Contate-nos através do nosso Centro de Suporte Online

Se não conseguir acessar as informações necessárias com o produto Bitdefender, por favor consulte o nosso Centro de Suporte online:

1. Vá para http://www.bitdefender.com/br/support/consumer.html.

   O Centro de Suporte doBitdefender armazena inúmeros artigos que contém soluções para as questões relacionadas ao Bitdefender.

2. Utilize a barra de pesquisa na parte superior da janela para encontrar artigos que possam fornecer uma solução definitiva para seu problema. Para pesquisar, apenas digite o termo na barra de pesquisa e clique em **Pesquisar**.

3. Leia os artigos ou os documentos e experimente as soluções propostas.

4. Se a solução não resolver seu problema, acesse

   http://www.bitdefender.com/br/support/contact-us.htmle contate nossos representantes de suporte.

31. RECURSOS ONLINE

Estão disponíveis vários recursos em linha para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte Bitdefender:

  http://www.bitdefender.com/br/support/consumer.html

- Fórum de Suporte Bitdefender:

  http://forum.bitdefender.com

- o portal de segurança informática HOTforSecurity:

  http://www.hotforsecurity.com

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

31.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, além de artigos mais gerais sobre prevenção de vírus, gestão de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é acessado com freqüência. A informção extensiva que ele contêm é mais um meio de proporcionar aos clientes do Bitdefender as informações técnicas e o conhecimento de que necessitam. Todos os pedidos de informação válidos ou relatórios de falhas oriundos de clientes do Bitdefender são eventualmente direcionados para o Centro de Apoio do Bitdefender, como relatórios de correção de falhas, fichas de resolução de problemas ou artigos informativos como suplemento dos arquivos de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer hora

http://www.bitdefender.com/br/support/consumer.html.

31.2. Fórum de Suporte Bitdefender

O Fórum de Suporte do Bitdefender proporciona aos utilizadores do Bitdefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto Bitdefender não estiver a funcionar correctamente, se não conseguir remover certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de suporte Bitdefender supervisionam o fórum à espera de novas mensagens para fornecer ajuda. Você também pode receber uma resposta ou solução de um usuário mais experiente do Bitdefender.

Antes de publicar o seu problema ou questão, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do Bitdefender está disponível em http://forum.bitdefender.com, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno. Clique na hiperligação **Protecção Casa & Casa/Escritório** para acessar à secção dedicada aos produtos de consumidor.

31.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui você pode conhecer as várias ameaças as quais seu computador fica exposto quando conectado à Internet (malware, phishing, spam, cibercriminosos).

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as actuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página web do HOTforSecurity é http://www.hotforsecurity.com.

32. INFORMAÇÃO SOBRE CONTATO

A comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível, excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

32.1. Endereços da Rede

Departamento de Vendas: vendas@bitdefender.com.br
Centro de Suporte:http://www.bitdefender.com/br/support/consumer.html
Documentação: documentation@bitdefender.com
Distribuidores locais:http://www.bitdefender.com/partners
Programa de parcerias: partners@bitdefender.com
Relações com a mídia: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Apresentação de Vírus: virus_submission@bitdefender.com
Envio de spam: spam_submission@bitdefender.com
Relato de abuso: abuse@bitdefender.com
Site Web:http://www.bitdefender.com

32.2. Distribuidores locais

Os distribuidores locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para http://www.bitdefender.com/partners/partner-locator.html.
2. Escolha seu país e cidade utilizando as opções correspondentes.
3. Se não encontrar um distribuidor Bitdefender no seu país, não hesite em contactar-nos por correio eletrônico através do endereço sales@bitdefender.com. Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

32.3. Escritórios Bitdefender

Os escritórios Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais. Seus endereços respectivos estão listados abaixo.

E.U.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefone (escritório&vendas): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Página da Web http://www.bitdefender.com

Alemanha

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Escritório: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://www.bitdefender.de/support/consumer.html
Página da Web http://www.bitdefender.de

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Fone: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: http://www.bitdefender.es/support/consumer.html
Website: http://www.bitdefender.es

Romênia

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefone de Vendas: +40 21 2063470
E-mail de vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/support/consumer.html
Website: http://www.bitdefender.ro

Emirados Arabes

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefone de Vendas: 00971-4-4588935 / 00971-4-4589186
E-mail de vendas: mena-sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Website: http://www.bitdefender.com

Glossário

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.

O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet.

Adware

O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disto, a informação que alguns destes programas coleta pode causar problemas de privacidade a usuários que não estão totalmente cientes do funcionamento do programa.

Ameaça persistente avançada

A ameaça persistente avançada (APA) explora as vulnerabilidades dos sistemas para roubar informações importantes e fornecê-las à fonte. Grandes grupos como organizações, empresas ou governos são os alvos deste malware.

O objetivo de uma ameaça persistente avançada é permanecer não detectada por um longo período, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas atacadas. O método usado para injetar o vírus na rede é através de um arquivo PDF ou documento do Office que pareça inofensivo, de forma que todo usuário possa abrir esses arquivos.

Área de Notificação

Introduzido com o Windows 95, a bandeja do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e acessar aos detalhes e controles.

Arquivo

Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.

Um arquivo que contém um ou mais arquivos em formato comprimido.

Arquivo de relatório

Um arquivo que lista as ações que ocorreram. Por exemplo Bitdefender mantém um arquivo de relatório com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos comprimidos verificados, quantos arquivos infectados e suspeitos foram encontrados.

Assinatura

Acordo de compra que dá ao usuário o direito de usar um produto ou serviço específico em um número específico de dispositivos e por um período de tempo determinado. Uma assinatura expirada pode ser automaticamente renovada usando a informação fornecida pelo usuário na primeira compra.

Assinatura de vírus

É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus.

Atualizar

Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador; caso contrário, você não poderá instalar a atualização.

O Bitdefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto.

Backdoor

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores ou mantenedores. A motivação para tais furos não pe sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante.

Caminho

As direções exatas de um arquivo em um computador. Estas direções são geralmente descritas por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores.

Cliente de e-mail

É um aplicativo que lhe permite enviar e receber e-mails.

Código de ativação

É um código exclusivo que pode ser comprado no varejo e usado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma assinatura válida por um determinado período de tempo e determinados dispositivos e também pode ser usado para estender uma assinatura com a condição de ser gerada para o mesmo produto ou serviço.

Cookie

Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem sendo analisados e usados pelos anunciantes para rastrear gostos e interesses on-line. Nesse contexto, a tecnologia de cookies ainda está em desenvolvimento e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma faca de dois gumes para muitos, porque por um lado é eficiente e pertinente porque só veja anúncios que interessam. E por outro lado, envolve "rastrear" e "seguir" a onde você vai e onde está clicando. Consequentemente, existe um debate sobre a privacidade e muitas pessoas se sentem ofendidas pelo fato de serem vistas como um número SKU (você sabe, o código de barras na parte traseira das embalagens que são lidas no caixa do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.

Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede.

E-mail

Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais.

Eventos

Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

Extensão do arquivo

É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: "c" para códigos em C, "ps" para PostScript, "txt" para texto.

Falso positivo

Ocorre quando a verificação identifica um arquivo infectado quando de fato não está.

Heurística

Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

IP

Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP.

Itens para inicializar

Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo, uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou um aplicativo pode ser um item de inicialização. Normalmente um pseudônimo deste arquivo é colocado nesta pasta, em vez do arquivo em si.

Java applet

Um programa em Java que é projetado para ser executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.

Por exemplo, mesmo que um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem.

Keylogger

Um keylogger é um aplicativo que registra tudo o que é digitado.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objetivos legítimos, tais como monitorar a atividade de funcionários ou crianças. No entanto, são cada vez mais usados por cibercriminosos com objetivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e CPF).

Linha de comando

Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem.

Não heurística

Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo pode parecer um vírus, e não gera falsos alarmes.

Navegador

Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Navegadores populares incluem o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plugins para alguns formatos.

Phishing

O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é solicitado a fornecer informações pessoais, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário.

Photon

Photon é uma tecnologia inovadora não-intrusiva da Bitdefender, projetado para minimizar o impacto da proteção antivírus no desempenho. Ao monitorar a atividade do seu PC em segundo plano, ele cria padrões de uso que ajudam a otimizar processos de inicialização e análise.

Porta

Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.

Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP.

Programas comprimidos

Um arquivo em formato compactado. Muitos sistemas operacionais e programas contêm comandos que permitem a você compactar um

arquivo para ocupar menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço consecutivos. Normalmente, isso requereria dez bytes de armazenamento.

Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Neste caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de compactação - existem muitas mais.

Ransomware

Ransomware é um programa malicioso que tenta lucrar com usuários através do travamento de seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem sistemas pessoais de usuários.

A infecção pode ser espalhada acessando um e-mail indesejado, baixando anexos de e-mail ou instalando aplicativos, sem que o usuário saiba o que está acontecendo em seu sistema. Usuários frequentes e empresas são alvos de hackers de ransomware.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, arquivos, logins e registros. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorar tráfego, criar backdoors no sistema, alterar arquivos e relatórios e evitarem ser detectados.

Script

Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário.

Setor de Boot

O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também contém um programa que carrega o sistema operacional.

Spam

Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado.

Spyware

Qualquer software que coleta informações do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.

A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia.

Deixando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho amplamente utilizado na Internet que permite comunicações em redes de computadores interconectadas com várias arquiteturas de hardware e diversos sistemas operacionais. O TCP/IP ínclui padrões de como os computadores se comunicam e convenções para conectar redes e direcionar o tráfego.

Trojan

Um programa destrutivo que oculta um aplicativo benigna. Ao contrário do vírus, um cavalo de tróia não se replica, mas pode ser muito destrutivo. Uma dos tipos mais incidentes de cavalos de tróia é um programa que afirma livrar seu computador de vírus, mas na verdade introduz vírus em seu computador.

O termo vem da história de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia.

Unidade de disco

É uma máquina que lê e escreve dados em um disco.

Uma unidade de disco rígido lê e escreve em um disco rígido.

Uma unidade de disquete acessa disquetes.

Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador).

Utilização de Memória

Áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips e a armazenagem de palavra é utilizada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente referida com memória RAM.

Virus

Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e é executado contra a sua

vontade. A maioria dos vírus pode também se duplicar. Todos os vírus de computador são feitos pelo homem. É fácil criar um simples vírus que pode se reproduzir repetidamente. Mesmo um simples vírus é perigoso, porque pode rapidamente usar toda memória disponível e fazer o sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

Vírus de boot

Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória.

Vírus de macro

Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitos aplicativos, como Microsoft Word e Excel, suportam poderosas linguagens de macro.

Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

Vírus polimórfico

Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar.

Worm

Um programa que se propaga pela rede, se reproduzindo enquanto avança. Ele não pode se anexar a outros programas.